(19)日本国特許庁（ＪＰ）　(12) **公表特許公報**（Ａ）　(11)特許出願公表番号

特表平11－511882

(43)公表日　平成11年(1999)10月12日

(51)Int.Cl.[6]		識別記号	ＦＩ		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｆ
	19/00		Ｇ１０Ｌ	3/00	５５１Ｐ
Ｇ０６Ｔ	7/00		Ｇ０６Ｆ	15/62	４６５Ａ
Ｇ１０Ｌ	3/00	５５１		15/30	３４０Ｃ

審査請求　未請求　　予備審査請求　有　　（全202頁）

(21)出願番号　特願平8－535098
(86)(22)出願日　平成８年(1996)５月17日
(85)翻訳文提出日　平成９年(1997)11月17日
(86)国際出願番号　ＰＣＴ／ＵＳ９６／０７１８５
(87)国際公開番号　ＷＯ９６／３６９３４
(87)国際公開日　平成８年(1996)11月21日
(31)優先権主張番号　０８／４４２，８９５
(32)優先日　1995年５月17日
(33)優先権主張国　米国（ＵＳ）

(71)出願人　スマート　タッチ，インコーポレイテッド
アメリカ合衆国　カリフォルニア　94704，バークレー，シャタック　スクエア　46，スイート　12
(72)発明者　ホフマン，ネッド
アメリカ合衆国　カリフォルニア　94704，バークレー，シャタック　スクエア　46，スイート　12
(72)発明者　ペア，デイビッド　エフ．
アメリカ合衆国　カリフォルニア　94704，バークレー，シャタック　スクエア　46，スイート　12
(74)代理人　弁理士　山本　秀策

最終頁に続く

(54)【発明の名称】　電子取引および電子送信の承認のためのトークンレス識別システム

(57)【要約】
トランザクションおよび送信を承認するためのトークンレス識別システムおよび方法が開示される。本発明によるトークンレスシステムおよび方法は、主として、未知のユーザ本人から直接、収集された、指紋や声紋記録のようなユニークなバイオメトリックサンプルを、以前に得られ格納された同一タイプの認証済みバイオメトリックサンプルと相関的に比較することに基づいている。本発明は、その他の独立したコンピュータシステム間の完全な、または部分的な仲立ちとして作用するようにネットワーク化されうるし、あるいは、必要なすべての実行事項をおこなう単独のコンピュータシステムであってもよい。また、本発明は、識別が完了し、そのコンピュータシステムがアクセスされたことをユーザに認証し、示した後に、ユーザに返送されるプライベートコードの使用も考慮に入れている。さらに、本発明による識別システムおよび方法は、承認されたユーザが、アクセスの企ては強要されたものであることを機関に警告することを可能にする緊急通知手段をさらに備えている。

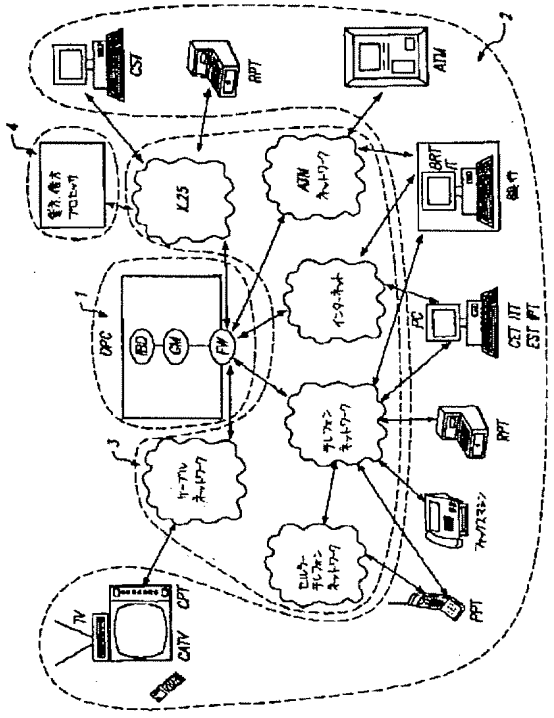

FIG. 1

【特許請求の範囲】

１．送信権要求ステップの間に収集された少なくとも１つのバイオメトリックサンプルおよび個人識別コードの検査と、登録ステップの間に収集され、以前に記録されたバイオメトリックサンプルおよび個人識別コードとの比較とによって個人の同一性を判定する、自発的なトークンレス識別コンピュータシステムであって、

ａ．少なくとも１つのコンピュータと、

ｂ．該登録ステップの間に、個人に、少なくとも１つのバイオメトリックサンプル、個人識別コード、およびプライベートコードを自発的に入力させる、第１の収集および表示手段であって、該プライベートコードが該個人により選択される、第１の収集および表示手段と、

ｃ．該送信権要求ステップの間に、個人に、少なくとも１つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第２の収集および表示手段と、

ｄ．該第１および該第２の収集および表示手段を該コンピュータに相互接続することによって、該収集されたバイオメトリックサンプル、該個人識別コードおよび該プライベートコードを該第１および該第２の収集手段から該コンピュータへと送信する、第１の相互接続手段と、

ｅ．該送信権要求ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードを、該登録ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードと比較することにより、評価を生じる手段と、

ｆ．データを格納し、コマンドを処理、実行することによって、判定を生じる、該コンピュータ内の実行手段と、

ｇ．該コンピュータから該評価、該判定あるいは該プライベートコードを出力する手段と、

を備えた自発なトークンレス識別コンピュータシステム。

２．前記第１および第２の収集および表示手段が、

ａ．ハードウェア部品およびソフトウェア部品をさらに有し、バイオメトリッ

クサンプルを収集する、少なくとも１つのバイオメトリック入力手段と、

ｂ．追加データを入力し、付加する、該バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも１つの端末手段と、

ｃ．個人識別コードを入力する少なくとも１つのデータ入力手段であって、該バイオメトリック入力手段または該端末手段のいずれか１つと一体化されている、データ入力手段と、

ｄ．該バイオメトリック入力手段、該データ入力手段および該端末を相互接続する、第２の相互接続手段と、

をさらに備えている、請求項１に記載の装置。

３．前記バイオメトリック入力手段が、前記コンピュータに対して以前に登録されたハードウェア識別コードを有しており、該ハードウェア識別コードが、該バイオメトリック入力手段を該コンピュータにとって固有のものとして識別可能とする、請求項２に記載の装置。

４．前記ハードウェア部品が、

ａ．データを処理する少なくとも１つのコンピューティングモジュールと、

ｂ．データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、

ｃ．バイオメトリックデータを入力するバイオメトリックスキャナ装置と、

ｄ．データを入力するデータ入力手段と、

ｅ．ディジタル通信ポートと、

ｆ．電子的盗聴を防止する手段と、

をさらに備えている、請求項２に記載の装置。

５．前記ハードウェア部品が、無線通信手段をさらに備えている、請求項２に記載の装置。

６．前記ソフトウェア部品がコンピューティングモジュール内に常駐しており、かつ

ａ．少なくとも１つのコマンドインタフェースモジュールと、前記バイオメトリック入力装置の意図的使用のために特に構成された、第１セットのソフトウェ

アおよび関連づけられたデータと、データとが格納されている、電子的に消去可能なメモリモジュールと、

ｂ．第２セットのソフトウェアおよび関連づけられたデータが格納される、非消去可能なメモリモジュールと、

をさらに備えている、請求項２に記載の装置。

７．前記ソフトウェア部品が、

ａ．平文から暗号文へとデータを暗号化する手段と、

ｂ．少なくとも１つのデバイスドライバと、

をさらに備えている、請求項８に記載の装置。

８．前記端末が、ファクシミリ機、電話、テレビジョンリモートコントロール、パーソナルコンピュータ、クレジット／デビットカードプロセッサ、キャッシュレジスタ、自動預金支払機および無線パーソナルコンピュータからなる群から選択される、請求項２に記載の装置。

９．前記比較手段が、前記バイオメトリック入力手段を識別する手段をさらに備えている、請求項１に記載の装置。

10．前記コンピュータシステムが、

ａ．少なくとも１つの独立したコンピュータネットワークシステムと

ｂ．該コンピュータシステムを相手側のコンピュータシステムに相互接続する

第３の相互接続手段と、

をさらに備えている、請求項１に記載の装置。

11．前記データベースが、個人バイオメトリックデータベースをさらに備えている、請求項13に記載の装置。

12．個人を自発的にトークンなしに識別し、該識別を認証する方法であって、

ａ．個人からの少なくとも１つのバイオメトリックサンプル、個人識別コードおよびプライベートコードが収集され、格納される、登録ステップと、

ｂ．個人からの少なくとも１つのバイオメトリックサンプルおよび個人識別コードが収集される、送信権要求ステップと、

ｃ．該送信権要求ステップの間に収集された該バイオメトリックサンプルおよ

び該個人識別コードが、該登録ステップの間に収集され格納された該バイオメトリックサンプルおよび該個人識別コードと比較されることにより、識別成功または識別失敗の結果を生じる、比較ステップと、

ｄ．コマンドが処理され実行されることによって、判定を生じる、実行ステップと、

ｅ．該識別結果または該判定が外面化され、表示される、出力ステップと、

ｆ．該個人の識別に成功するとただちに、該プライベートコードが該識別されている該個人へと提示される、提示ステップと、

を含む方法。

13．アカウントインデックスが緊急アカウントとしてラベルが付けられ、該アカウントがアクセスされた場合には、該緊急時が適切な機関に通知される、緊急アカウントインデックス割り当てステップをさらに含んでいる、請求項12に記載の方法。

14．前記登録ステップおよび前記送信権要求ステップが、前記データを平文から暗号文へと変換する暗号化ステップをさらに含んでいる、請求項12に記載

の方法。

15．前記送信権要求ステップまたは前記登録ステップには、ユニークなハードウェア識別コードを有し、送信の度に１ずつ増加するシーケンスナンバをインクリメントする、ユニークな送信コードがさらに設けられている、請求項12に記載の方法。

16．前記比較ステップが、反復送信を検出するのに前記ユニークな送信コードを使用することを含む、請求項12に記載の方法。

17．前記比較ステップが、相手側の識別コードおよび前記ユニークな送信コードを用いる相手側識別ステップをさらに含む、請求項12に記載の方法。

18．前記比較ステップが、前記送信権要求ステップの間に収集された前記個人の前記個人識別コードおよび前記バイオメトリックスを、前記登録ステップの間に収集された前記個人識別コードおよび前記バイオメトリックスと照合することにより、該個人を肯定的に識別することを含む、請求項12に記載の方法。

19. 前記実行ステップが、借受／貸付トランザクションステップをさらに含む、請求項12に記載の方法。

20. 前記実行ステップが、アーカイブ化ステップと、データをアーカイブするトラッキングコード割り当てステップとをさらに含む、請求項12に記載の方法。

21. 前記提示ステップが、前記プライベートコードを外面化することをさらに含む、請求項12に記載の方法。

22. 第１の個人からの少なくとも１つの以前に格納された第１のバイオメトリックサンプルを、個人識別コードバスケットを用いて迅速にサーチする方法において、該個人識別コードバスケットが、該個人識別コードバスケットにより識別される少なくとも１人の第２の個人からの少なくとも１つのアルゴリズム的にユニークな第２のバイオメトリックサンプルを含みうる、方法であって、

ａ．格納ステップであって、

ｉ．該第１の個人による個人識別コードの選択と、

ii．該第１の個人からのバイオメトリックサンプルの入力と、

iii．該第１の個人により選択された該個人識別コードにより識別された該個人識別コードバスケットの位置を特定することと、

iv．該第１の個人から取られた該バイオメトリックサンプルを、該選択された個人識別コードバスケット内に以前に格納されたバイオメトリックサンプルのいずれかと比較することにより、該第１の個人により入力された該バイオメトリックサンプルが、少なくとも１人の第２の個人により提供され、以前に格納された少なくとも１つのバイオメトリックサンプルと比べてアルゴリズム的にユニークであることを確かめることと、

ｖ．もし該サンプルが、該少なくとも１人の第２の個人からの該少なくとも１つの以前に格納されたバイオメトリックサンプルと比べてアルゴリズム的にユニークであるのなら、該第１の個人からの該入力されたバイオメトリックサンプルを該選択された個人識別コードバスケットに格納することと、

を含む、格納ステップと、

ｂ．送信権要求ステップであって、

ｉ．該第１の個人により該選択された個人識別コードを入力することと、

ii．該第１の個人によりバイオメトリックサンプルを入力することと、

を含む、送信権要求ステップと、

ｃ．比較ステップであって、

ｉ．該第１の個人により入力された該個人識別コードにより識別される該個人識別コードバスケットを検索することと、

ii．該第１の個人からの該入力されたバイオメトリックサンプルを、該入力された個人識別コードバスケットにおける該少なくとも１人の第２の個人からの該

少なくとも１つの格納されたバイオメトリックサンプルと比較することにより、識別成功または識別失敗のいずれかの結果を生じることと、

をさらに含む、比較ステップと、

を含む方法。

23．送信権要求ステップの間に収集された少なくとも１つのバイオメトリックサンプルおよび個人識別コードの検査と、登録ステップの間に収集され以前に記録されたバイオメトリックサンプルおよび個人識別コードとの比較と、によって個人の同一性を判定する、自発的なトークンレス識別コンピュータシステムであって、

ａ．少なくとも１つのコンピュータと、

ｂ．該登録ステップの間に、個人に、少なくとも１つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第１の収集および表示手段と、

ｃ．該送信権要求ステップの間に、個人に、少なくとも１つのバイオメトリックサンプルおよび個人識別コードを自発的に入力させる、第２の収集および表示手段と、

ｄ．該第１および該第２の収集および表示手段を該コンピュータに相互接続することによって、該収集されたバイオメトリックサンプルおよび該個人識別コードを該第１および該第２の収集手段から該コンピュータへと送信する、第１の相互接続手段と、

ｅ．該送信権要求ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードを、該登録ステップの間に収集された該バイオメトリックサンプルおよび該個人識別コードと比較することにより、評価を生じる手段と、

ｆ．データを格納し、コマンドを処理、実行することによって、判定を生じる、該コンピュータ内の実行手段と、

ｇ．該コンピュータから該評価または該判定を出力する手段と、

を備えた自発的なトークンレス識別コンピュータシステム。

24．前記第１および第２の収集および表示手段が、

ａ．ハードウェア部品およびソフトウェア部品をさらに有し、バイオメトリックサンプルを収集する、少なくとも１つのバイオメトリック入力手段と、

ｂ．追加データを入力し、付加する、該バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも１つの端末手段と、

ｃ．個人識別コードを入力する少なくとも１つのデータ入力手段であって、該バイオメトリック入力手段または該端末手段のいずれか１つと一体化されている、データ入力手段と、

ｄ．該バイオメトリック入力手段、該データ入力手段および該端末を相互接続する、第２の相互接続手段と、

をさらに備えている、請求項23に記載の装置。

25．前記バイオメトリック入力手段が、前記コンピュータに対して以前に登録されたハードウェア識別コードを有しており、該ハードウェア識別コードが、該バイオメトリック入力手段を該コンピュータにとって固有のものとして識別可能とする、請求項24に記載の装置。

26．前記ハードウェア部品が、

ａ．データを処理する少なくとも１つのコンピューティングモジュールと、

ｂ．データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、

ｃ．バイオメトリックデータを入力するバイオメトリックスキャナ装置と、

ｄ．データを入力するデータ入力手段と、

ｅ．ディジタル通信ポートと、

ｆ．電子盗聴を防止する手段と、

を備えている、請求項24に記載の装置。

27．前記ハードウェア部品が、無線通信手段をさらに備えている、請求項24に記載の装置。

28．前記ソフトウェア部品がコンピューティングモジュール内に常駐しており、かつ

ａ．少なくとも１つのコマンドインタフェースモジュールと、前記バイオメトリック入力装置の意図的使用のために特に構成された、第１セットのソフトウェアおよび関連づけられたデータと、データとが格納されている、電子的に消去可能なメモリモジュールと、

ｂ．第２セットのソフトウェアおよび関連づけられたデータが格納される、非消去可能なメモリモジュールと、

をさらに備えている、請求項24に記載の装置。

29．前記相互接続手段が、無線通信用の手段である、請求項24に記載の装置。

30．前記比較手段が、前記バイオメトリック入力装置を識別する手段をさらに備えている、請求項23に記載の装置。

31．前記コンピュータシステムが、

ａ．少なくとも１つの相手側コンピュータシステムと、

ｂ．該コンピュータシステムを該相手側コンピュータシステムに相互接続する第３の相互接続手段と、

をさらに備えている、請求項23に記載の装置。

32．個人を自発的にトークンなしに識別し、該識別を認証する方法であって、

ａ．個人からの少なくとも１つのバイオメトリックサンプルおよび個人識別コードが収集され、格納される、登録ステップと、

ｂ．個人からの少なくとも１つのバイオメトリックサンプルおよび個人識別コードが収集される、送信権要求ステップと、

ｃ．該送信権要求ステップの間に収集された該バイオメトリックサンプルおよ

び該個人識別コードが、該登録ステップの間に収集され格納された該バイオメトリックサンプルおよび該個人識別コードと比較されることにより、識別成功または

は識別失敗の結果を生じる、比較ステップと、

ｄ．コマンドが処理され実行されることによって、判定を生じる、実行ステップと、

ｅ．該識別結果または該判定が外面化され表示される、出力ステップと、

を含む方法。

33．アカウントインデックスが緊急アカウントとしてラベルが付けられ、該アカウントがアクセスされた場合には、該緊急時が適切な機関に通知される、緊急アカウントインデックス割り当てステップをさらに含んでいる、請求項32に記載の方法。

34．前記登録ステップおよび前記送信権要求ステップが共に、データの改変を検出する能力を提供するデータ隠蔽ステップをさらに含んでおり、

ａ．秘密鍵と、

ｂ．該秘密鍵なしには再生されえない該データの非可逆的一方向変換と、

を含む、請求項32に記載の方法。

35．前記比較ステップが、反復送信を検出するのに前記ユニークな送信コードを使用することをさらに含む、請求項32に記載の方法。

36．前記比較ステップが、前記送信権要求ステップの間に収集された前記個人の前記個人識別コードおよび前記バイオメトリックスを、前記登録ステップの間に収集された前記個人識別コードおよび前記バイオメトリックスと照合することにより、該個人を肯定的に識別することを含む、請求項32に記載の方法。

【発明の詳細な説明】

電子取引および電子送信の承認のためのトークンレス識別システム

背景

今日の金融界ではトークンおよびクレジットカードの使用が広く普及している。トークンは何らかの無生物であり、これを提示する個人に、権限をあたえるものである。金融口座への遠隔アクセスはすべてトークンまたはプラスチックカードを用いて行われる。デビットカード（debit card）で食品雑貨を購入する場合も、クレジットカードで消費財を購入する場合も、その取引の中心にあるのは、個人と、個人がアクセスしている金融口座とを識別する役割を果たすクレジットカードまたは「スマートカード（smart card）」などのトークンによって可能となる金銭の移動である。残念なことに、この便利なトークンベースの金銭移動システムと組み合わせた現在の技術で得られたシステムは、盗みおよび詐欺が起こりやすいシステムである。

ユーザ同一性の検証は、個人間で容易に再生できかつやりとりできるトークンにあるデータのみに基づいて行われ、そのような場合の安全性は、承認されたユーザおよびマーチャントがこの情報を所有物として維持する際の努力と運とをあてにしなければならないものである。しかし、トークンは、その本質により、個人とあまり強い関連があるわけではない。トークンの正当な所有者の識別はどうみても十分ではない。このことは、トークンの正当な所有者以外の個人がこれらのトークンを用いてマーチャントおよび他の消費財供給者に詐欺行為をはたらいていることから容易に証明される。

このシステムがその性質上非常に無防備であるため、クレジット業界では多くの様々な地域で詐欺による損害が起こっているが、この損害は主に、紛失したカード、盗まれたカード、あるいは偽造カードによるものである。クレジッドカードは個人識別コード（personal identification code）（ＰＩＣ）を使用しなければ使えないため、紛失カードが他人の手に渡った場合、カードを現金に換えることができる。ジステムの詐欺の大部分がトークンを盗むことにより起こっているため、偽造クレジットカードの使用が増加し続けている。クレジットカードは

より高度な技術を持つ者によって偽造されており、カード保有者の有効な口座番号を得て、この有効な番号を用いて偽造カードを作っている。偽造者は、磁気ストリップを符号化し、偽造プラスチックカードに口座番号を打ち出す（emboss）。このカードをマーチャントに提示すると、正当なカード保有者の口座に支払いが請求される。他の形態の損害は、マーチャントがカード保有者の口座番号を不正に利用するという犯罪行為によって起こる損害である。さらに、承認されたカード保有者がトークンを用いて買い物をし、その後にトークンを紛失したあるいは盗まれたとして申請するというタイプの詐欺もある。すべてのタイプの詐欺による損害は年間９億５０００万ドルを越えると推定される。

一般に、デビットカードは個人識別コード（ＰＩＣ）とともに用いられる。デビットカードの偽造は、口座番号だけではなくＰＩＣも知る必要があり、それを知って初めてカードを作ることができるため、クレジットカードの場合よりも困難である。しかし、様々な戦略を用いて、不注意なカード保有者からＰＩＣを得ており、この戦略には、ショッピングモールにあり、現金を分配するがＰＩＣを記録するトロイの木馬のように危険な現金自動預け払い機（automated teller machine）すなわちＡＴＭから、これもＰＩＣを記録するマーチャント用販売時点情報管理（ＰＯＳ）デバイス、およびカード保有者がＡＴＭでＰＩＣを入力するのを双眼鏡で見る人といったものがある。その後に偽造したデビットカードを様々なＡＴＭ機で用いてその不運な口座が空になるまで使うのである。

この偽造詐欺のため、産業界では、過去１０年間にわたって、クレジットカード取引システムの使用については根本的な変更はせずにトークンを変更した。この対処法は、顧客に自分のカードをアクティベートするように発行者に依頼してもらうといった主に管理上の変更であった。他の変更としては、ホログラム、写真ＩＤ、または改良を加えた署名領域の追加がある。これらのタイプの変更は特に、システムで個人の真の識別がなされていないために詐欺が容易であることを示している。これらの変更を行えば、製造コストが年間20億ドルに倍増すると推定される。

銀行業界は、近い将来、「スマートカード」と呼ばれるさらに高価なカードに

移行するであろうと予測している。スマートカードは、最初のホームコンピュータのうちの幾つかのものが持っていた計算力と同等の計算力を含む。第１世代のスマートカードの現在のコスト見積は、流通コストを除いて約３．５０ドルであると推定され、これは、プラスチックカードブランクの０．３０ドルよりもかなり高い。

電子金融取引の普及に加えて、およびその普及に伴って、現在では、電子ファクシミリ、電子メールメッセージおよび同様の電子通信が広く用いられている。個人が適切に識別されないという金融取引に関する問題点と同様に、電子送信に関しても個人が適切に識別されないという問題点がある。電子通信は、その簡便さおよび速度ならびに従来の郵便よりも低いコストによって、似通った個人およびビジネス間におけるえり抜きの通信方法となった。しかし、ファクシミリおよび電子メール（または、「Ｅ－メール」もしくは「ｅメール」）などの非常に多くの電子メッセージの場合、それを送ってもそれが真の宛先に届いているかどうか、または特定の個人が実際にその電子メッセージを送信もしくは受信したかどうかは分からない。さらに、電子メッセージを送信または受信した個人の識別名（identify）を確かめる方法がない。

以上のことに鑑みて、詐欺が非常に起こりにくく、実用的で、ユーザが迅速に電子取引および電子伝送を操作しかつ実行するのに効率的なコンピュータアクセスシステムが長い間必要とされている。

個人が個人間で自由にやりとりできる何らかの物理的なものを所有しているかどうかを検証するのではなく、承認されたユーザに固有で身体的に個人的なものであるバイオメトリクスと、個人識別コードとのみに基づいてユーザの個人識別名を検証することができるコンピュータシステムも必要とされている。

特に、多数のまたは厄介なコードを覚える必要性を大幅に少なくするまたはなくし、アクセスリクエストを開始するために所有者の財産物（proprietary object）を所有し、携帯し、提示する必要性をなくす金融取引システムが必要とされている。

さらに、ユーザが、多数の口座にアクセスし、ユーザに対して承認されたすべてのサービスを獲得し、すべての金融口座における取引およびすべての金融口座

間の取引を行い、購入品の支払いを忘れずに行い、様々なサービスを受けることができるようにするコンピュータシステムも要求されている。

さらに、このコンピュータシステムは、様々な電子取引デバイス、電子送信デバイス、およびシステム構成を有する既存のネットワークと動作的に互換性があるほど十分に柔軟で、手頃なものでなければならない。

最後に、電子メールメッセージおよび電子ファクシミリが安全に送信および受信され、電子メッセージの内容が承認されていない個人に漏れないように保護され、送り手または受け手の識別名を高い確実性で得ることができるようにする必要がある。

発明の要旨

本発明は、送信権要求ステップの間に収集された個人のバイオメトリックサンプルおよび個人識別コードを、その個人について、登録ステップの間に収集され、データ処理センターのある遠隔サイトに格納されたバイオメトリックスサンプルおよび個人識別コードと比較することによって個人の同一性を判定する、改善された識別システムを提供することによって、これらの要求を満たす。本発明は、入力されたバイオメトリックサンプルおよび個人識別コードを比較する手段を備え、さまざまなデータバスおよびメモリモジュールを備えた、コンピュータネットワークホストシステムを備えている。また、本発明は、バイオメトリックスおよび個人識別コード入力装置と、いったん個人の同一性が判定された後、要求されたトランザクションおよび送信をホストシステムにより実行する情報を提供するためのデータ入力端末と、を備えている。また、本発明は、ホストシステムを、端末およびバイオメトリックス入力装置に接続する手段をも備えている。

コンピュータは、また、従来のデータ格納および変更と共に、さまざまなトランザクションおよび送信を実行する手段も備えている。さらに、コンピュータは、バイオメトリックス－ＰＩＣ（「個人識別コード」）の比較の評価、およびトランザクションまたは送信の何らかの実行について、識別評価またはステータスの判定を出力することができる。また、コンピュータシステムは、登録ステップの間に個人により以前に選択された秘密コードをその個人に返送することによって、

そのコンピュータシステムがアクセスされたことを、現在、識別されている個人に通知し、そのことを認証する。

好ましくは、このコンピュータシステムは、電子的盗聴および電子的侵入およびウイルスから保護される。バイオメトリックサンプルおよび個人識別コードを収集するためにこのコンピュータにより用いられる装置は、ａ）ハードウェア部品およびソフトウェア部品を有し、バイオメトリックサンプルを収集する、少なくとも１つのバイオメトリック入力装置と、ｂ）補助データを入力し、付加する、バイオメトリック入力手段と機能的にその一部または全部が一体化された、少なくとも１つの端末装置と、ｃ）個人識別コードを入力する少なくとも１つのデータ入力装置であって、バイオメトリック入力装置または端末装置のいずれか１つと一体化されている、データ入力装置と、ｄ）バイオメトリック入力装置、データ入力装置および端末を相互接続する手段と、を備えている。この端末装置は、また、データおよび情報を表示する少なくとも１つの表示装置を備えている。さらなるセキュリティを保証するために、このコンピュータシステムは、バイオメトリック入力装置を固有のものとして識別し、バイオメトリック入力装置に接続されている端末に関わる相手側の識別コードすなわちマーチャント識別コードを通して、相手側すなわちマーチャントを固有のものとして識別する。また、好ましくは、このバイオメトリック入力装置は物理的および電子的改変から保護されており、この装置が物理的に侵害された場合には、その装置内の部品を物理的および／または電子的に破壊し、および／または装置のメモリモジュールから重要なデータを消去する手段が用いられる。

加えて、このバイオメトリック入力装置は、データ処理モジュールと、データおよびソフトウェアを格納する消去可能メモリモジュールおよび非消去可能メモリモジュールと、バイオメトリックデータを入力するバイオメトリックスキャナ装置と、データを入力するデータ入力装置と、ディジタル通信ポートと、を備えたハードウェア部品を備えている。

バイオメトリック入力装置、端末およびコンピュータネットワーク間で送られた電子的データの完全性および秘匿性を保護するためには、このデータは暗号化され、シールされるのが好ましい。

ホストコンピュータシステムは、また、その他の独立したコンピュータシステム、データベース、ファクシミリ機、およびその他のネットワークと、従来の手段を介して接続されており、それらと通信することができる。

本発明の方法は、個人により提供された少なくとも１つのバイオメトリックサンプルと、やはりその個人により提供された個人識別コードとを検査することにより、トークンを全く用いず、自発的に個人を識別することを含む。登録ステップにおいて、個人は、システムに対して、認証されたバイオメトリックサンプルと、個人識別コードと、秘密コードとを登録することが求められる。その後、送信権要求ステップにおいて、この個人のバイオメトリックスサンプルおよび個人識別コードが収集され、登録ステップの間に登録されたものと比較される。個人識別コードおよびバイオメトリックスサンプルが一致すると、その個人が肯定的に識別される。現実のコンピュータシステムにアクセスされたことを識別された個人に認証するために、登録ステップにおいて集められた個人の秘密コードは、個人に返送される。

本発明の方法は、好ましくは、登録の間にバイオメトリックスサンプルを検査し、以前に悪事を企てたとして指定されている個人、または実際に詐欺によりシステムに悪事を働いた個人から集められたバイオメトリックスサンプルと、そのようなバイオメトリックスサンプルとを比較する方法を含む。

好ましい実施の形態では、本発明は、緊急状況の存在、または承認されたユーザが脅迫されていることを機関に通知する方法を含む。

また、ファクシミリまたは電子メールメッセージのような何らかの文書が、その文書を将来識別するためのアルゴリズムを用いて、固有のものとしてチェックサムされるのも好ましい。

本発明のさらに別の方法は、異なる複数の個人からのいくつかの類似していないバイオメトリックスサンプルを、ある個人識別コードにより識別される電子バスケットに格納し、個人のバイオメトリックスサンプルおよび個人識別コードを検査することによって、その個人を迅速に識別することができる。

本発明のある実施の形態では、コンピュータシステムは、各個人が、遠隔データ処理センターにより選択された１グループの個人識別コード（「ＰＩＣ」）か

ら

自らのＰＩＣを選択することを可能にする。これは、いったん個人のバイオメトリックが収集されると、データ処理センターが、記憶するにふさわしい（condustive to）いくつかのＰＩＣをランダムに選択する方法においておこなわれる。その後、データ処理センターは、収集されたこれらのバイオメトリックと、ＰＩＣバスケットまたはグループに既に存在しているバイオメトリックとの比較をおこなう。新規登録者のバイオメトリックが、これらのランダムに選択されたＰＩＣグループのいずれか１つに対して割り当てられ、以前に登録されたバイオメトリックと類似している場合には、そのＰＩＣは、新しい個人により使用されるデータベースにより拒絶され、別のそのようなバイオメトリック比較をおこなうために、代わりのＰＩＣが選択される。いったんデータ処理センターが、いくつかの類似したバイオメトリックスを混同することなく、いくつかのＰＩＣオプションを発生した後、これらのＰＩＣは、新規登録者に提示され、個人は、そこから１つのＰＩＣを選択することができる。

本発明のある実施の形態では、第１の個人からの少なくとも１つの以前に格納された第１のバイオメトリックサンプルを、個人識別コードバスケットを用いて迅速にサーチする方法において、個人識別コードバスケットが、上記個人識別コードバスケットにより識別される少なくとも１人の第２の個人からの少なくとも１つのアルゴリズム的にユニークな第２のバイオメトリックサンプルを含みうる、方法が提供される。この方法は、まず、格納ステップであって、ａ）第１の個人による秘密コードの選択と、ｂ）上記第１の個人による個人識別コードの選択と、ｃ）上記第１の個人からのバイオメトリックサンプルの入力と、ｄ）上記第１の個人により選択された個人識別コードにより識別された個人識別コードバスケットの位置を特定することと、ｅ）上記第１の個人から取られたバイオメトリックサンプルを、上記選択された個人識別コードバスケット内に以前に格納されたバイオメトリックサンプルのいずれかと比較することにより、上記第１の個人により入力されたバイオメトリックサンプルが、少なくとも１人の第２の個人により提供され、以前に格納された少なくとも１つのバイオメトリックサンプルと

比べてアルゴリズム的にユニークであることを確かめることと、ｆ）もし上記サンプルが、上記少なくとも１人の第２の個人からの上記少なくとも１つの以前に格納

されたバイオメトリックサンプルと比べてアルゴリズム的にユニークであるのなら、上記第１の個人からの入力されたバイオメトリックサンプルを選択された個人識別コードバスケットに格納することと、を含む、格納ステップを含む。また、送信権要求ステップであって、ａ）上記第１の個人により上記選択された個人識別コードを入力することと、ｂ）上記第１の個人によりバイオメトリックサンプルを入力することと、を含む、送信権要求ステップをも含む。さらには、比較ステップであって、ａ）上記第１の個人により入力された上記個人識別コードにより識別される個人識別コードバスケットを検索することと、ｂ）上記第１の個人からの入力されたバイオメトリックサンプルを、上記入力された個人識別コードバスケットにおける上記少なくとも１人の第２の個人からの上記少なくとも１つの格納されたバイオメトリックサンプルと比較することにより、識別成功または識別失敗のいずれかの結果を生じることと、を含む、比較ステップをも含む。また、ａ）コマンドが処理され実行されることによって、判定を生じる、実行ステップと、ｂ）上記識別結果または上記判定が外面化され表示される、出力ステップと、ｃ）上記第１の個人の識別に成功するとただちに、上記秘密コードが上記第１の個人へと提示される、提示ステップと、をも含む。

本発明のある実施の形態によれば、ホストシステムは、識別されている個人と、アクセスされるべき別のコンピュータネットワークとの間に直列に位置づけられることによって、インタフェースとして作用する。なお、この実施の形態において、ユーザは、ＶＩＳＡＮＥＴのような他の独立し安全の保証されたコンピュータシステムと動作的にインタラクティブである、本発明によるホストコンピュータシステムへと直接、アクセスリクエストを提出することは理解されたい。よって、このコンピュータシステムは、それがサービスする安全の保証されたコンピュータシステムそれぞれのすべての承認済みユーザについて認証されたバイオメトリックデータサンプルを維持する。これらのデータは、承認済みユーザ各人

により相互参照される。よって、同一性の検証が終了した後、セキュリティシステムは、ユーザに対して、ユーザがアクセスを承認されているシステムのリストを提供し、ユーザに対して所望のネットワークを選択するようプロンプトする。その後、リクエストされた実行ステップおよびトランザクションに関する情報は、今日、マ

ーチャントとクレジットカード会社との間でやりとりされている通信と似たタイプの選択された独立コンピュータネットワークへと送出される。

第２の実施の形態では、ホストシステムは、また、例えば、金融アカウントから借り受けたり、そこへ貸し付けたりすることのような、その他の独立したコンピュータシステムの機能を実行することもできる。このシステムでは、本発明のコンピュータシステムは、外部の独立したコンピュータネットワークを用いずに、個人によりリクエストされた機能を実行する。

本発明によるさらに別の実施の形態によれば、ホストコンピュータシステムへのアクセスをリクエストするサードパーティによりユーザが強要されているアクセスの企ての間に、予め指定された機関へと警告を発する手段が提供される。このような実施の形態では、承認されたユーザは、いくつかのコードをもつことになる。これらのコードの大半は、コンピュータシステムにより標準的アクセスコードとして認識されることになるが、他のものは、緊急コードとして認識されることになる。本発明のコンピュータシステムの比較手段は、承認されたユーザ１人につき少なくとも１つのコードを受け入れ、認識するように構成されており、ユーザにより入力されたコードが緊急コードと一致する時にはいつでも、緊急警告手段を作動させるように構成される。同時に、ユーザについて承認済みの同一性が判定されると、おそらくは制約されるように予め定められたアクセスレベル、またおそらくはミスリーディングデータ（すなわち「偽の画面」）が表示される結果となるアクセスレベルにおいて、リクエストされた安全の保証されたコンピュータシステムへのアクセスがそのユーザに許される結果となる。これにより、ユーザにより緊急通知が入力されたことを、強要者のサードパーティが知るのを防止できる。緊急コードは、ユーザの個人識別コードの一部として、あるいは

それと同時に入力されるか、またはコンピュータシステムへのアクセス時に緊急アカウントインデックスを選択することによって入力される。いずれの場合にせよ、アクセスをリクエストするユーザの利益は、もしそのユーザが機関への通知を企てていたことを強要者であるサードパーティが知ったのなら、危険にさらされることになる。

本発明は、いくつかの点で、明らかに従来技術よりもすぐれている。第１に、

ユーザにとって、特にユーザが金融アカウントにアクセスしようとしている時には、本発明は、きわめて簡単で、効率がよい。なぜなら、人は、アカウントにアクセスするのに、トークンをもっていることも提示することも必要なくなるからである。本発明は、要求された何らかのトークンを携帯し、安全保護し、その在処を突き止めることに関わるあらゆる不便をなくす。また、トークンは、特定のトークンに割り当てられた秘密コードを覚えていることをさらに要求する特定のコンピュータシステムに固有であることがよくあるので、本発明は、そのようなトークンを一切排除し、ただ１つの個人識別コードを用いてすべての資産へのアクセスを実現することによって、消費者にますます要求されている記憶および義務励行の量を大幅に減らすことができる。よって、一回限りのトークンレストランザクションで、消費者は、銀行アカウントからの現金の引き出しから、契約条項へと同意することを認めること、テレビジョンから直接、購入すること、さらには固定資産税の支払いに至るまで、ほとんどありとあらゆる商業的やりとりまたは電子的メッセージのやりとりを効率よく、かつ安全に実行することができる。

このような電子トランザクションは、また、操作コストを大幅に削減することによって、マーチャントおよび銀行が、大量の時間および出費を節約することを可能にする。本発明のシステムは、消費者が自らのもつ金融アカウントのすべてに対して同時に直接、アクセスすることを可能にするように設計されているので、金銭、小切手、商業書類その他を伴うトランザクションの必要性は大幅に低くなり、それにより、このようなトランザクション用の設備コストおよび収集・計算に必要なスタッフを減らすことができる。また、クレジットカード、ＡＴＭカ

ード、名刺などを発行し、再発行するための実質的な製造コストおよび配布コストをなくすことができるので、マーチャント、銀行ひいては消費者にとってさらに経済的な節約が可能になる。

本発明は、ユーザの１つ以上のユニークなバイオメトリックス特徴の分析に基づきユーザの同一性を判定することによって、非承認ユーザにアクセス権を賦与する危険性を実質的に排除することができる。

また、本発明は、認証データを維持し、ユーザのリクエストしているアクセスからは操作的に分離されたシステムにおける一点で同一性検証操作を実行することによって、詐欺に対する抵抗力をさらに強化し、それにより、ユーザが、認証データのコピーを取ったり、検証プロセスを改変したりするのを防止することができる。このようなシステムは、例えば、パーソナルコードのような認証情報がトークンに基づいて格納され、トークンから復元されうることになっており、かつ実際の同一性判定が、アクセスプロセス中にユーザと操作を通じてコンタクトを取っておこなわれる可能性のある、現存のトークンに基づくシステムよりも明らかに優れている。

よって、本発明の目的は、システムアクセスリクエストを開始するに当たって、ユーザが、例えばトークンのような物理的オブジェクトを所有し、提示する必要がないようにするコンピュータアクセス識別システムを提供することにある。

本発明の別の目的は、所有物および所有情報の所有を検証するのではなく、ユーザの同一性を検証できるコンピュータアクセス識別システムを提供することにある。

本発明のさらに別の目的は、ユーザにとって物理的に個人独特のものである１つ以上のユニークな特性に基づいて、ユーザの同一性を検証することにある。

ユーザにより提供された所望のコンフィギュレーションに従って、コンピュータシステム上でユーザのトランザクション能力を自動的に制約するコンピュータアクセス識別システムもまた必要とされている。本発明の上記利点およびその他の利点は、添付の図面と併せて、以下に述べる本発明の詳細な説明を読めば、さらに明らかになるであろう。

図面の簡単な説明

図１は、本発明のシステムの図である。

図２は、データプロセシングセンター（ＤＰＣ）およびその内部データベースおよび実行モジュールの図である。

図３は、小売ＰＯＳターミナル、バイオメトリックス入力装置およびその構成要素、およびそれらの間の相互接続の図である。

図４は、リクエストパケットを生成するための、バイオメトリックス入力装置およびターミナルの動作のフローチャートである。

図５は、リクエストパケットおよびそれが包含する必須およびオプショナルデータを描写した図である。

図６は、レスポンスパケットおよびそれが包含する必須およびオプショナルデータを描写した図である。

図７は、バイオメトリックス入力デバイスにおける、データ暗号化およびシーリングプロセスを表すフローチャートである。

図８は、ＤＰＣにおけるデータ復号化およびカウンタパーティ識別プロセスを表すフローチャートである。

図９は、ＤＰＣにおけるデータ暗号化およびシーリングプロセスを表すフローチャートである。

図１０は、登録プロセス中の個人の登録を表すフローチャートである。

図１１は、個人の識別および個人へプライベートコードを返すプロセスを示すフローチャートである。

図１２は、ＤＰＣおよびある実行ステップで起こるプロセスの概略のフローチャートである。

図１３は、ＤＰＣにおける緊急リクエストおよびレスポンスプロセスのフローチャートである。

図１４は、ＤＰＣにおける小売トランザクション承認実行動作の全体のフローチャートである。

図１５は、ＤＰＣにおける遠隔トランザクション承認実行動作の全体のフローチ

ャートである。

図１６は、ＤＰＣにおけるＡＴＭアカウントアクセス実行動作の全体のフローチャートである。

図１７は、ＤＰＣにおける発行者バッチ改変実行動作の全体のフローチャートである。

図１８は、ＤＰＣにおける安全なファックス入力および電子文書入力実行動作の全体のフローチャートである。

図１９は、ＤＰＣにおける安全なファックスデータおよび電子文書データ実行動作の全体のフローチャートである。

図２０Ａは、電子署名リクエストパケットを描写した図である。

図２０Ｂは、電子署名レスポンスパケットを描写した図である。

図２０Ｃは、電子署名検証リクエストパケットを描写した図である。

図２０Ｄは、電子署名検証リクエストパケットを描写した図である。

図２１は、ＤＰＣにおける電子署名実行動作の全体のフローチャートである。

図２２は、ＤＰＣにおける電子署名検証実行動作の全体のフローチャートである。

発明の詳細な説明

このように、本発明の主な目的は、金融取引および金融以外の伝送を行うことを目的とした、個人を識別するための、多くのユーザーに対応できる、トークンレス装置および方法を提供することである。消費者が、いかなるトークン、クレジットカード、バッジ、あるいは運転免許証を含む身分証明書を使用することなく、これらの取引を遂行することができる、ということが、本発明の本質である。システムは、複数の銀行やクレジットアカウント（credit accounts）から、クレジットカードによる購入やＡＴＭサービスのような金融取引を完了するのに必要な速度で動作する。本システムは安全であるので、個人の記録およびバイオメトリックス情報は、個人を識別し、取引を承認するコンピューターシステム内においても、またコンピュータシステムとそのコンピューターシステムが通信する遠隔地との間のデータ転送中においても、機密かつ安全なままである。さらに

、このシステムは、識別および承認における誤りが、システムの使用を阻害したり、扱いにくくしたりしてはいけないという点において、信頼性がある。個人の識別には、バイオメトリックスの使用のみが想定されているので、システムには、緊急の場合には、承認されたユーザーに対してでさえ、アクセスを削減したり、当局（authorities）に通報したりする安全対策が講じられている。

ここで図を見ることにする。本発明の全体的な構成およびその構成要素が図１に示されている。基本的に、データプロセシングセンター（ＤＰＣ）１は、いくつかのタイプの内の１つであり得る、様々なタイプの通信手段３によって、様々なターミナル２に接続されている。ＤＰＣはまた、独立したコンピュータネットワーク４に接続され、これと通信する。ＤＰＣは、図２に示すように、いくつか

のデータベースおよびソフトウェア実行モジュールを含む。発明の好適な実施形態では、データベースは、安全保護のため、バックアップされるか「ミラーリング」されている。ファイアウォールマシン５はシステムの電子的侵入を防止する役割を果たしているのに対し、ゲートウェイマシン６は全データベースの追加、削除およびその他の改変を含む、ユーザーからのすべてのリクエストを実行する役割を果たしている。ゲートウェイマシンはまた、ＭＡＣＭモジュール７、ＭＤＭモジュール８、およびＳＮＭモジュール９を用いたターミナルから届いたデータを復号およびデパッケージ（de-packaging）する役割も果たす。ＰＧＬモジュール１０およびＩＭＬモジュール１１は、適切な個人識別コードおよびバイオメトリックスサンプルバスケットを見つけるために使用される。図３はターミナルおよびバイオメトリックススキャナー１３、キーパッドあるいはＰＩＮパッド１４のようなデータ入力手段および表示パネル１５を有するバイオメトリックス入力デバイス１２の一例を示している。バイオメトリックススキャナーは、指紋スキャナー、音声認識、掌紋スキャナー、網膜スキャナー等のいずれでもあり得るが、指紋スキャナーを例として使用する。バイオメトリックス入力デバイスはさらに、コンピューティングモジュール１６、デバイスドライバ、および消去可能および消去不可能メモリモジュールを備えている。バイオメトリックス入力デバイスは、好適にはシリアルポート１７を通してターミナルと通信する。ターミナ

ル２は、従来のモデム１８、リクエストパケット１９およびレスポンスパケット２０を通し、ケーブルネットワーク、セルラー電話ネットワーク、電話ネットワーク、インターネット、ＡＴＭネットワーク、あるいはＸ．２５のような、図１の相互接続手段の１つを用いてＤＰＣ１と通信する。図４は、リクエストパケット１９およびバイオメトリックス入力デバイスソフトウェアによるその生成方法を描写した図である。図５および図６は、オプショナルおよび必須のデータセグメントを有するリクエストパケットおよびレスポンスパケットを描写した図である。さらに、パケットのどの部分が暗号化されており、どの部分がシールされているかも示されている。図７は、データの暗号化およびシーリングの全体的なプロセスのブロック図であり、メッセージ認証コードキー（ＭＡＣ）２１を用いたリクエストパケットシーリング前の、追加データ付加前の、データ暗号化用のＤ

ＵＫＰＴキーデータ２０の使用を示している。図８および図９は、ＤＰＣでの復号化および暗号化プロセスを示している。図１２から１９および２１から２２は、ＤＰＣで続行される実行ステップの選択例のブロック図である。

図面、図、フローチャートの説明、およびハードウェア構成要素、ソフトウェア構成要素、実行モジュール、データベース、接続手段、それらの間で転送されたデータを含む本発明の説明、および本発明の方法の説明を、以下で詳細に行う。

バイオメトリック入力装置（ＢＩＡ）

ＢＩＡは、個人の識別に使用するためのバイオメトリック入力を収集、コード化および暗号化することをそのジョブとするハードウェアおよびソフトウェアの組み合わせである。ＢＩＡのすべてのアクションは、ターミナルと呼ばれる外部の制御エンティティ（controlling entity）によって指令され、これはＢＩＡのシリアルライン上でコマンドを発行し、結果を受け取る。

ＢＩＡのハードウェアには４つの基本バージョン、すなわち、標準、ワイヤレス、一体型電話／ケーブルテレビ（すなわち「ＣＡＴＶ」）／ファックス、およびＡＴＭがある。ＢＩＡハードウェアの各変形体は、市場の特定のニーズに対処し、構成に相違があるため、各変形体のセキュリティのレベルは異なる。

ＢＩＡソフトウェアには７つの基本バージョン、すなわち、パーソナルコンピュータ（すなわち「ＰＣ」）、小売、ＡＴＭ、登録、インターナル（internal），発行者，および集積型リモート（integrated remote）がある。各ソフトウェアをロードすると、異なった、特定の用途のためのコマンドのセットが提供される。例えば、登録ソフトウェアをロードすると、小売トランザクションのメッセージを形成するリクエストは受け付けられない。同様に、小売ソフトウェアのコマンドセットは個人の登録メッセージを送ることはできない。別のセキュリティ層を提供するために、ＤＰＣは各ＢＩＡにどのソフトウェアパッケージがロードされているかを知っており、ＢＩＡによる、通常送ることのできないメッセージを送ろうとする試みはいかなるものであれ拒絶され、重大なセキュリティ違反として扱われる。

ＢＩＡの外付けインターフェースは厳しく限定されているため、ＢＩＡの構成

により、そのコンテンツを不正改変することは極度に困難になる。さらに各ＢＩＡは、ＤＰＣしか知らない固有の暗号化コードを持っており、各ＢＩＡはそれに指定された機能に限定された動作しか行えないようになっている。各バイオメトリック入力手段は、ＤＰＣに予め登録されたハードウェア識別コードを有しており、このためバイオメトリック入力手段は、そのバイオメトリック入力デバイスからの後続する各転送において、ＤＰＣにとって一意に識別できるものとなる。

ターミナルのレンジは、パーソナルコンピュータ上で動作するソフトウェアアプリケーションから、小売ＰＯＳのような特定の用途に開発された専用ハードウェア／ソフトウェアシステムにまで至る。特定のモデルにかかわらず、暗号化されていないバイオメトリック情報を漏らすＢＩＡはない。表示手段のないＢＩＡモデル（例えばＬＣＤ、ＬＥＤあるいはクォーツスクリーン）は、表示用ターミナルに、選択された情報（例えば個人プライベートコード）を明らかにしなければならず、その結果、それらの特定のターミナル－ＢＩＡの組み合わせは、安全性が劣ると考えられている。

当面のタスクにより、ＢＩＡモデルは、部分的にあるいは完全にターミナルと一体化される。部分的に一体化されているデバイスは、ターミナルと物理的に離

れており、それらはワイヤレスおよび標準小売ＰＯＳのＢＩＡを含む。完全に一体化されたデバイスは、例えばＡＴＭや電話のようなターミナル自体に物理的に包含されている。ＢＩＡは、いかなる外部のソースにであれ、秘密の暗号化コードを明らかにすることはない。

ＢＩＡモデル

具体的なＢＩＡハードウェアモデルは、異なる構成を有する。以下にそれらを簡単に紹介する。

ＢＩＡ

標準モデルは、演算モジュール（すなわち、マルチチップモジュール）、バイオメトリックスキャナ（すなわち、単一の指紋スキャナ）、表示手段（すなわち、ＬＣＤスクリーン）、通信ポート（すなわち、シリアルポート）、不正改変不可能

なケースの中に包まれたデータエントリ手段（すなわち、マニュアルデータエントリキーボードまたはＰＩＣパッド）、および電子検出手段（すなわち、ＲＦシールド）を有する。

ＢＩＡ/ワイヤレス

標準モデルであって、シリアルラインが、外部アンテナを用いる広スペクトル（spread-spectrum）ワイヤレス通信モジュールに置き換わった標準モデル。レストランＰＯＳ（point of sale）において用いられる。

ＢＩＡ/ＡＴＭ

マルチチップモジュールと共に、ヘビーデューティスキャナおよびシリアルポートを有する。ＬＤＣがターミナルの一部であってＢＩＡ手段の一部ではないという事実は、セキュリティを低下させる。なぜなら、ＬＣＤは、秘密コードをターミナルへ知らせなければいけないから。ＡＴＭにおいて用いられる。

ＢＩＡ/Ｃａｔｖ

ライトデューティスキャナを有する。それ以外はＡＴＭと同様である。電話、ＣＡＴＶリモート、およびファクスマシンにおいて用いられる。ＬＣＤおよびＰＩＣパッドがターミナルの一部であってＢＩＡの一部ではないために、さらに市

場の低コスト性（low-cost nature）のために、最もセキュリティが弱い。

ＢＩＡコマンドセットメッセージ

それぞれのＢＩＡソフトウェアコマンドセットは、動作の異なるセットを提供する。以下にそれらを簡単に紹介する。

ＢＩＡ/ＡＴＭ

アカウントアクセス（Ａccount Ａccess）

ＢＩＡ/Ｃatv

遠隔取引承認（Ｒemote Ｔransaction Ａuthorization）

ＢＩＡ/ファクス

安全ファクス提出（Ｓecure Ｆax Ｓubmit）

安全ファクスデータ（Ｓecure Ｆax Ｄata）

安全ファクス追跡（Ｓecure Ｆax Ｔracking）

安全ファクス取り出し（Ｓecure Ｆax Ｒetrieve）

安全ファクス拒否（Ｓecure Ｆax Ｒeject）

安全ファクスアーカイブ（Ｓecure Ｆax Ａrchive）

安全ファクス契約受諾（Ｓecure Ｆax Ｃontact Ａccept）

安全なファクス契約拒否（Ｓecure Ｆax Ｃontact Ｒeject）

電子ドキュメントアーカイブ取り出し（Ｅlectronic Ｄocument Ａrchive Retrieve）

ＢＩＡ/内部

個人の識別（Ｉndividual Ｉdentification）

ＢＩＡ/発行者

発行者バッチ（Ｉssure Ｂatch）

ＢＩＡ/ＰＣ

電子ドキュメント提出（Ｅlectronic Ｄocument Ｓubmit）

電子ドキュメントデータ（Ｅlectronic Ｄocument Ｄata）

電子ドキュメント追跡（Ｅlectronic Ｄocument Ｔracking）

電子ドキュメント取り出し（Ｅlectronic Ｄocument Ｒetrieve）

電子ドキュメント拒否（Ｅlectronic Document Reject）

電子ドキュメントアーカイブ（Ｅlectronic Document Archive）

電子ドキュメントアーカイブ取り出し（Ｅlectronic Document Archive Retrieve）

電子署名サブミッション（Ｅlectronic Ｓignature Ｓubmission）

電子署名チェック（Ｅlectronic Ｓignature Ｃheck）

遠隔取引承認（Ｒemote Ｔransaction Ａuthorization）

ネットワーククレデンシャル（Ｎetwork Ｃredential）

保護された接続（Ｓecured Ｃonnection）

ＢＩＡ/登録

個人の識別（Ｉndividual Ｉdentification）

バイオメトリック登録（Ｂiometric Ｒegistration）

ＢＩＡ/小売

取引承認（Ｔransaction Ａuthorization）

ＩＡハードウェア：標準モデル

標準ＢＩＡハードウェアは、固い不正改変不可能なケースの中に包まれた単一のプリントスキャナ、ＬＣＤスクリーン、シリアルポート、およびＰＩＣパッドと組み合わされたマルチチップモジュールである。固い不正改変不可能なケースは、コンテンツのためのＲＦシールドを提供するとともに、侵入する企てを明白にさせる。

次のコンポーネンツは、ＢＩＡマルチチップモジュール（当該分野において公知な、いくつかのプロセッサを一つの物理シェルに閉じ込めるためのプロセス）と呼ばれるマルチチップモジュールに合併されている。マルチチップモジュールは、デバイス間の通信経路を簡単な傍受から防護するように構築されている。

・シリアルプロセッサ

・ＰＩＣパッドプロセッサ

・ＬＣＤスクリーンプロセッサ

・ＣＣＤスキャナＡ/Ｄプロセッサ

・フラッシュおよびマスクＲＯＭの両方を含む高速ＤＳＰプロセッサ

・汎用マイクロプロセッサ

・標準ＲＡＭ

・ＥＥＰＲＯＭ

次のソフトウエアパッケージおよびデータは、マスクＲＯＭに記憶されている。マスクＲＯＭは、読み出し専用メモリの他のタイプよりも安価であるが、しかしリバースエンジニアされやすく、そして電子的に消去することができない。そのようなものとして、ここでは重要でない一般に利用可能なコードを並べるにとどめる。（マスクＲＯＭは当該分野において公知である）。

・ＭＡＣ計算ライブラリ

・ＤＵＫＰＴ鍵管理ライブラリ

・ＤＥＳ（ＣＢＳともに）暗号化ライブラリ

・Base-64（８ビットから印刷可能なＡＳＣＩＩへの）コンバータライブラリ

・公開鍵暗号化ライブラリ

・埋込みオペレーティングシステム

・シリアルラインデバイスドライバ

・ＬＣＤデバイスドライバ

・ＰＩＣパッドデバイスドライバ

・スキャナデバイスドライバ

・ユニークハードウエア識別（identification）コード

・マルチ－言語プロファイル

次の標準データおよびソフトウエアパッケージはフラッシュＲＯＭにおいて記憶される。フラッシュＲＯＭは、より高価であるが、リバースエンジニアすることがさらにより困難であり、そして最も重要なことだが、電子的に消去可能である。より重要な情報の全てはここに記憶される。フラッシュＲＯＭは、ＢＩＡを複製することの困難さを増加させる試みで用いられる。（フラッシュＲＯＭは、当該分野において公知である）。

・ユニークＤＵＫＰＴ未来鍵（future key）テーブル

・ユニーク112－ビットＭＡＣ鍵

・ＤＳＰバイオメトリック品質（biometric quality）決定アルゴリズム

・ＤＳＰバイオメトリックコード化（encoding）アルゴリズム

・乱数発生アルゴリズム

・コマンドファンクションテーブル

ＢＩＡからメッセージが送られる毎にインクリメントされるメッセージシーケンス番号は、ＥＥＰＲＯＭにおいて記憶される。ＥＥＰＲＯＭは、何回も消去されてもよいが、しかし非揮発性である－そのコンテンツは、電源の遮断を越えて有効のままである。（ＥＥＰＲＯＭは、当該分野において公知である）。

次のデータはＲＡＭにおいて記憶されている。ＲＡＭは、性質上一時的であり、電源が失われた場合は、いつでも失われる。

・コード化されたバイオメトリックレジスタ（Encoded Biometric Register）

・ＰＩＣレジスタ（ＰＩＣ Register）

・アカウントインデックスコードレジスタ（Acount Index Code Register）

・タイトルインデックスコードレジスタ（Title Index Code Register）

・アマウントレジスタ（Amount Register）

・ドキュメント名レジスタ（Document Name Register）

・ＰＩＣ－ブロック鍵（ＰＩＣ-Block Key）

・メッセージ鍵（Message Key）

・レスポンス鍵（Response Key）

・共有セッション鍵（Shared Session Key）

・秘密セッション鍵（Private Session Key）

・８汎用レジスタ（８ General Registers）

・スタックおよびヒープ空間（stack and heap space）

それぞれのマルチチップモジュールは、フラッシュＲＯＭの初期化に続いて不可逆にセットされる「一度の書き込み（write-once）」メモリロケーションを含

む。フラッシュＲＯＭへソフトウエアをダウンロードする試みが行われた場合にはいつでも、このメモリロケーションはチェックされる。もし、それがすでにセットされていたならば、その後、ＢＩＡはロードすることを拒否する。この方法で、重要なソフトウエアおよびデータ鍵は、製造時に一度だけ、デバイスにダウンロードされうる。

次の関連するハードウエアコンポーネンツは、標準ＢＩＡハードウエアモジュールを備える。

・ＢＩＡマルチチップモジュール（ＢＩＡ Multichip module）

・ＣＣＤシングループリントスキャナ（ＣＣＤ single-print scanner）

・容量検出板（capacitance detector plate）（当該分野において公知）

・照明されたＰＩＣキーパッド（lighted ＰＩＣ keypad）

・２－ライン40－カラムＬＣＤスクリーン（２-line 40-column ＬＣＤ screen）

・ＲＦシールド（ＲＦ shielding）

・不正改変不可能なケース（tamper-resistant case）

・シリアルコネクション（57.6kbまで）（serial connection）

・ブリーチ検出ハードウエア（breech detection hardware）（当該分野において公知）

・マルチチップモジュールに取り付けられた、選択可能なテルミットチャージ（thermite charge）（当該分野において公知）

これらの値を計算するために用いられる、全ての一時記憶手段および内部ハードウエアおよびソフトウエアは、保護される。このことは、それらが、それらの現在の値、または機能に関するそれらの意味を決定するいかなる試みにも耐える。この特徴は、この発明のセキュリティにとって本質的てある。ＢＩＡの「傍受」や、そして特に、不正手段のためのバイオメトリック－ＰＩＣブロックの収集が可能な限り困難にされることが、まさに重要だからである。

マルチチップモジュールとコンポーネンツとは、実際には、露出した配線が存在することなく、物理的に接続されている。

ＢＩＡの電子コンポーネンツを防護しているエンクロージャーは、製造中に溶接されて蓋をされる。それは、ケースへの重大なダメージなしでは、いかなる状況下でも開けられ得ない。エンクロージャーのいかなる開封（またはダメージ）を

検出した際には、ＢＩＡは、フラッシュＲＯＭにある、いかなる全ての鍵について緊急電子的ゼロ（emergency electronic zero）を実行し、その次に、ソフトウエアライブラリの全てついて実行する。特定のブリーチ（breech）検出メソッドは、極秘かつ独占（Proprietary）を維持される。

コンテンツを防護することに加えて、ケースは、ＲＦ信号検出器から、内部動作をシールドする。

ＢＩＡの超安全な（supersecure）バージョンが存在し、それによってブリーチ（breech）検出メソッドは、検出メソッドそれ自体だけでなくマルチチップモジュールをも物理的に破壊する機構に接続されている。

ＢＩＡハードウエア：ワイヤレスモデル

ＢＩＡハードウエアのワイヤレスバージョンは、それが、外部シリアルポートの代わりに、外部アンテナを用いた広スペクトルワイヤレス通信モジュールをエクスポートすることを除いて、構造上標準モデルと同じである。

このバージョンは、レストランにおいて用いられるように設計されている。レストランでは、顧客の都合に合わせて、取引が承認される。

次の記述において、標準セットに追加されるアイテムは、＋文字によって表記される。一方、標準セットから除去されるアイテムは、－文字によって表記される。

マルチチップモジュール：

・ドキュメント名レジスタ（Document Name Register）

・共有セッション鍵（Shared Session Key）

・秘密セッション鍵（Private Session Key）

・メッセージ鍵（Message Key）

コンポーネンツ：

・シリアルポート（Ｓerial port）

・外部アンテナ（Ｅxternal antenna）

・広スペクトルワイヤレスシリアルモジュール（当該分野において公知）

ＢＩＡハードウエア：ＡＴＭ（自動テラーマシン）モデル

ＢＩＡハードウエアのＡＴＭバージョンは、ヘビーデューティシングループリントスキャナ（heavy-duty single-print scanner）とシリアルポートとに結合されたマルチチップモジュールである。コンポーネンツは、不正改変不可能なケースの中に包まれる。不正改変不可能なケースは、コンテンツのためのＲＦシールドを提供するとともに、侵入する企てを明白にさせる。

このバージョンは、ＡＴＭの位置において改装されるように設計される。そのようなものとして、スキャナパッドは、ヘビーデューティセンサパッドであり、全体の構造は、ＡＴＭそれ自体において存在するスクリーンおよびキーパッドを利用する。

次の記述において、標準セットに追加されるアイテムは、＋文字によって表記される。一方、標準セットから除去されるアイテムは、－文字によって表記される。

マルチチップモジュール：

・アマウントレジスタ（Ａmount Ｒegister）

・ドキュメント名レジスタ（Ｄocument Ｎame Ｒegister）

・共有セッション鍵（Ｓhared Ｓession Ｋey）

・秘密セッション鍵（Ｐrivate Ｓession Ｋey）

・メッセージ鍵コンポーネンツ：（Massage Ｋey Ｃomponents:）

・照明されたＰＩＣキーパッド（lighted ＰＩＣ keypad）

・２－ライン40－カラムＬＣＤスクリーン（２-line 40-column ＬＣＤ screen）

ＡＴＭはＬＣＤスクリーンまたはＰＩＣキーパッドを有さないので、実は、マスクＲＯＭにおいてそれらのデバイスドライバが必要ないことに注意されたい。

ＢＩＡハードウエア：電話／ＣＡＴＶモデル

ＢＩＡハードウエアの電話／ＣＡＴＶバージョンは、シングループリントスキャナ

（single-print scanner）とシリアルポートとに結合されたマルチチップモジュールである。モジュールは、物理的にスキャナに取り付けられており、全体は、干渉を行うのをより困難にするために、プラスチックの中に包まれている。かなりの量のＲＦシールドがコンポーネンツのために提供される。

このバージョンは、電話機、テレビジョンリモートコントロールおよびファクスマシンと一体化されるように設計される。結果として、それは、存在するキーパッド、ＬＣＤまたはテレビジョンスクリーンを利用して、値をエンターまたは表示する。また、それはホストターミナルの通信機能を使う。例えば、ファクスマシンはビルトインファクスモデムを用い、テレビジョンリモートは、ＣＡＴＶケーブルネットワークを用いる。

このハードウエアモデルは、（他のモデルと比較して）比較的安全性が低い。それらのデバイスが、可能な限りコストがかからず、軽重量であり、存在する低コストデバイスと容易に一体化できるように意図されるからである。

次の記述において、標準セットに追加されるアイテムは、＋文字によって表記される。一方、標準セットから除去されるアイテムは、－文字によって表記される。

マルチチップモジュール：

・ドキュメント名レジスタ（Document Name Register）

・共有セッション鍵（Shared Session Key）

・秘密セッション鍵（Private Session Key）

・メッセージ鍵（Message Key）

コンポーネンツ：

・照明されたＰＩＣキーパッド（lighted ＰＩＣ keypad）

・２－ライン40－カラムＬＣＤスクリーン（2-line 40-column ＬＣＤ screen）

ＢＩＡソフトウエア

ＢＩＡソフトウエアコマンドインターフェイス

ＢＩＡへの外部インターフェイスは、標準モデムによく似ている。外部シリアルラインを用いて、コマンドが制御ターミナルからＢＩＡに送られる。コマンドが完了した場合、レスポンスコードがＢＩＡからターミナルへ送られる。

それぞれのＢＩＡソフトウエアロード（software load）は、動作の異なるセットをサポートする。例えば、小売ロード（retail load）は、取引承認だけをサポートし、一方、登録ロード（registration load）は、個人の識別（identification）およびバイオメトリック登録をサポートする。

全てのＢＩＡデータフィールドは、プリント可能なＡＳＣＩＩの形態であり、fs制御文字で分離されたフィールド、および復帰改行（newlines）によって分離されたレコードとを有する。暗号化されたフィールドは、base-64変換ライブラリを用いて64－ビットＡＳＣＩＩに変換されたバイナリである（これらは当該分野において公知である）。

いくらかのコマンドは、いくらかの構成において利用できない。例えば、ＡＴＭＢＩＡは、「Get ＰＩＣ」できない。なぜなら、ＰＩＣパッドが取り付けられていないから。そのかわり、ＡＴＭＢＩＡは、「Set ＰＩＣ」コマンドをサポートする。

レスポンスコード：

時間切れ：

コマンドに割り当てられた時間が満了した。その効果に対するメッセージが、ＬＣＤスクリーンが利用可能ならば、それ上に表示される。所定のコマンドに対して時間が満了した場合、ＢＩＡは、キャンセルボタンが押されたかのように動作する。

キャンセルされた：

キャンセルボタンが押され、そして全動作がキャンセルされた。これは、集められた全ての情報を取り除くという副効果を有する。その効果に対するメッセージが、ＬＣＤスクリーンが利用可能ならば、それ上に表示される。

Ok：

コマンドが成功した。

その他：

それぞれのコマンドが、それに対してのみ有効な、特定の他のレスポンスコードを有してもよい。これらのレスポンスコードは一般に、コードに付随するテキストを有してもよい。テキストは、ＬＣＤスクリーンが利用可能ならば、それ上に表示される。

メッセージ：

これは、コマンドが進行中であることを示し、しかしＢＩＡがターミナルに中間結果のメッセージを送りたいことを示す。この結果は、また、ＬＣＤスクリーンが利用可能ならば、それ上に表示される。この機能は、ステータスメッセージだけでなくプロンプトのためにも用いられる。

コマンド

以下のコマンドの引数（argument）リストにおいて、〈〉の文字で個々の引数を囲み、[]の文字でオプショナルな引数を囲み、｜の文字は、ある引数が示された選択肢のうちの１つからなり得ることを示す。

Set language〈言語名〉

このコマンドは、ユーザ入力を促す（prompt）ための、ＢＩＡ内で符号化される複数の異なる言語のうち１つを選択する。

Get Biometric〈時間〉［１次｜２次］

このコマンドは、ＢＩＡに、そのスキャナを作動させて、個人からバイオメトリック入力を得て、符号化バイオメトリックレジスタに格納することを要求する。

まず、「点灯したパネル上に指をおいて下さい」のメッセージがＬＣＤパネル上に表示され、ターミナルに返される。スキャナパッドが照明されて、個人がそのバイオメトリックをエンターするように促す。

〈時間〉値がゼロであることは、バイオメトリックスキャン入力に時間制限がないことを意味する。

スキャニングモードにおいて、指紋スキャンがとられ、紋品質アルゴリズム(p

rint quality algorithm)によって予備分析がなされる。スキャンが十分よくない場合は、ＢＩＡは〈時間〉秒が経過するまで新しいスキャンをとり続ける。時間が経過して紋のスナップショットがとられて分析されると、メッセージがＬＣＤスクリーンに掲示されて、紋品質ソフトウェアによって検知された問題に基づきターミナルに送られる。適切な品質の紋が得られない場合は、ＢＩＡは時間が過ぎたことを示すエラーコードを返し、その旨のメッセージをＬＣＤ上に表示する。

紋品質アルゴリズムが紋スキャンの品質を是認(affirm)すると、紋の詳細(minutiae)が紋符号化アルゴリズムによって抽出される。識別に十分な量を保持するように注意しながら、詳細の部分集合のみをランダムに選択する。次に詳細をランダムに並べ、符号化バイオメトリックレジスタに入れる。すると、ＢＩＡは成功結果コードでもって応答する。

もし［１次｜２次］が指定されていれば（バイオメトリック登録コマンドセットにおいてのみ利用可能）詳細セットの小さな部分集合だけでなくその全体が選択される。同様に、１次／２次バイオメトリック選択は、符号化されたバイオメトリックを適切なレジスタに入れることになる。

動作が成功するか否かに関わらず、スキャニングが終わるとともに、スキャニングが進行中であることを示すライトが消灯される。

同じバイオメトリック入力が異なる符号結果（encoding）を生みだすことにより、手に入れた（capture）ＢＩＡの暗号化コードを発見しようとする者の作業を複雑にすることが非常に重要である。これは、ランダムな部分集合を選択し、符号化バイオメトリックをランダムに並べることにより、達成される。

Get PIC〈時間〉

このコマンドは、ＢＩＡがキーパッドからの読み取りを行うことによってＰＩＣレジスタを埋めることを要求する。

まず、「あなたのＰＩＣを入力してから〈エンター〉を押して下さい」のメッセージがＬＣＤディスプレイ上に表示されてターミナルに送られ、適切なキーパッドライトが点灯され、次にキーパッドスキャニングが開始される。

〈時間〉秒数が切れたときか、個人が〈エンター〉キーを押したときに、スキャニングが終了する。

ＰＩＣの個々の数字はＬＣＤ上に表示されす、個々がタイプする各数字に対して星印「*」が現れることにより個人にフィードバックを行う。「訂正」キーが押されたとき、最後にエンターされた数字が消去され、個人が入力ミスを直すことを可能にする。

ＰＩＣ入力が終了すると、キーパッドライトが消灯する。

成功すれば、コマンドはＯＫを返す。

Get Account Index Code〈時間〉

まず、「ではあなたのアカウントインデックスコードを入力してから〈エンター〉を押して下さい」のメッセージがＬＣＤ上に表示されてターミナルに送られる。これにより、個人は自分のアカウントインデックスコードをエンターするように促される。各キーが押されたとき、その値がＬＣＤパネル上に現れる。訂正ボタンをおすことによって値のうち１つを消去することかできる。「エンター」ボタンが押されると、アカウントインデックスコードレジスタがセットされる。

入力中、適切なキーパッドのキーが点灯され、入力が完結したとき、キーパッドのライトが消灯される。

成功すれば、コマンドはＯＫを返す。

Get Title Index Code〈時間〉

まず、「あなたのタイトルインデックスコードを入力してから〈エンター〉を押して下さい」のメッセージがＬＣＤ上に表示されてターミナルに送られる。これにより、個人は自分のタイトルインデックスコードをエンターするように促される。各キーが押されたとき、その値がＬＣＤパネル上に現れる。訂正ボタンをおすことによって値のうち１つを消去することができる。「エンター」ボタンが

押されると、タイトルインデックスコードレジスタがセットされる。

入力中、適切なキーパッドのキーが点灯され、入力が完結したとき、キーパッドのライトが消灯される。

成功すれば、コマンドはＯＫを返す。

Validate Amount〈金額〉〈時間〉

Validate Amountコマンドは、「金額〈金額〉ＯＫ？」のメッセージをターミナルに送り、これをＬＣＤスクリーン上に表示する。もし個人が「はい」（またはエンター）ボタンを押すことにより金額を確認すれば、金額レジスタが〈金額〉にセットされる。〈金額〉値は、制御文字やスペースなどの無い、有効な数字でなればならない。プロンプトを出している間、はい、いいえ、およびキャンセルボタンが点灯される。プロンプトが完了すると、全てのライトが消灯される。

もし個人が「いいえ」をエンターすると、トランザクションはキャンセルされる。

Enter Amount〈時間〉

Enter Amountコマンドは、「金額を入力して下さい」のメッセージをターミナルに送り、これをＬＣＤスクリーン上にも表示する。個人は次にドル金額を自分でエンターしなければならない。エンターされた各文字は、ＬＣＤスクリーン上に表示される。全ての適切なボタンが点灯される。エンターボタンが押されると、金額レジスタがキーボード上でエンターされた値にセットされる。入力が完了すると、全てのライトが消灯される。

Validate文書〈名称〉〈時間〉

Validate Documentコマンドは、「文書〈名称〉ＯＫ？」のメッセージをターミナルに送り、これをＬＣＤスクリーン上にも表示する。もし個人が「はい」（またはエンター）ボタンを押すことにより文書を確認すれば、文書名レジスタが〈名称〉にセットされる。〈名称〉値は、制御文字や前後のスペースなどの無い、印刷可能なASCII文字でなればならない。プロンプトを出している間、はい、

いいえ、およびキャンセルボタンが点灯される。プロンプトが完了すると、全てのライトが消灯される。

もし個人が「いいえ」をエンターすると、トランザクションはキャンセルされる。

Assign Register〈レジスタ〉〈テキスト〉

assign registerコマンドは、指定された一般〈レジスタ〉を値〈テキスト〉

を有するようにセットする。これは、マーチャントコード、製品情報などの情報をセットするために用いられる。

Get Message Key

Get Message Keyコマンドは、ＢＩＡに、制御装置がメッセージに追加したい任意のメッセージ本体を暗号化するために制御ハードウェアが使用する、５６ビットランダム鍵を生成させる。生成された鍵は、１６進数フォーマット（当該分野では公知）でＢＩＡに返される。メッセージ鍵が次にバイオメトリック－ＰＩＣブロックに追加される。

Form Message〈タイプ識別｜トランザクション｜アカウントアクセス...〉

Form Messageコマンドは、ＢＩＡに、集めた全ての情報を含むメッセージを出力するように命令する。また、その特定のメッセージ〈タイプ〉に適切な全てのレジスタがセットされたことを確実にするためチェックする。もし全てのレジスタがセットされていなければ、ＢＩＡはエラーを返す。特定のコマンドセットソフトウェアが、そのＢＩＡモデルによってどのメッセージが形成され得るかを決定し、その他は全て拒否される。

各メッセージは、ＢＩＡの固有のハードウェア識別コードからなる送信コードおよび、インクリメントするシーケンス番号を含んでいる。送信コードは、送っているＢＩＡをＤＰＣが識別し、再入力攻撃(resubmission attack)を検知することを可能にする。

ＢＩＡは、ＤＵＫＰＴ鍵管理システムを用いて、将来鍵テーブルからバイオメトリック－ＰＩＣブロック暗号化５６ビットＤＥＳ鍵を選択する。この鍵は次に、暗号化ブロックチェイニング（ＣＢＣ）(cipher block chaining)を用いてバイオメトリック－ＰＩＣブロックを暗号化するために使用される。また、レスポンスＤＥＳ鍵もランダムに生成され、レスポンスの中で暗号化される必要のある部分を暗号化するためにＤＰＣによって使用される。

注：レスポンス鍵をバイオメトリック－ＰＩＣブロック鍵は、非常に重要である。なぜなら、各暗号化鍵はその責任範囲でのみ使用されなければならないからである。このようにすれば、もし何者かが秘密コードを符号化している鍵を破ろ

うとしても、バイオメトリック－ＰＩＣの露呈には至らない。

ＢＩＡ－ＰＩＣブロックの構成フィールド：

・３００バイト承認バイオメトリック

・４－１２桁ＰＩＣ

・５６ビットレスポンス鍵

・［オプショナルな５６ビットメッセージ鍵］

メッセージ鍵は、制御ターミナルがこのメッセージに対するメッセージ鍵を要求した場合にのみ存在することに注意せよ。メッセージ鍵を用いてトランザクション承認リクエストに添付されたメッセージ本体の暗号化は、制御ターミナルに委ねられる。

全ての暗号化が完了すると、ＢＩＡは、メッセージ承認コード（ＭＡＣ）によって終了かつ保護される、適切なリクエストメッセージ（例えばトランザクション承認リクエストメッセージなど）の本体を出力する。

ＭＡＣフィールドは、ＢＩＡのシークレット１１２ビットＤＥＳＭＡＣ鍵を用いて計算され、１番目から最後までの全てのメッセージフィールドをカバーする。ＭＡＣは、制御ターミナルが平文フィールドを検査(inspect)することを可能にしながら、メッセージ内に、効果的にメッセージを密封することを変更するものは何もなかったことを、ＤＰＣに対して保証する。

Form Messageコマンドが実行されると、ＢＩＡは、「ＤＰＣ中央と通話しています」のメッセージをターミナルに送り、ＬＣＤスクリーンにもこれを表示し、作業がリクエストに対して進行中であることを示す。

コマンドが完了すると、コマンドは、形成されたメッセージ全体を返すとともにＯＫを返す。

Show Response〈暗号化レスポンス〉〈時間〉

Show Responseコマンドは、ＢＩＡに、その現在のレスポンス鍵を用いてシステムから秘密コードを復号化するように命令する。

復号化後、チャイムが鳴り、秘密コードがＬＣＤスクリーンに〈時間〉秒間表示される。このコマンドは、復号化された秘密コードを制御ターミナルに送信す

ることは、いかなる時点においてもない。

Validate Private〈復号化された有効性証明〉〈時間〉

このコマンドは、安全なネットワーク通信セッション中において、個人に外部ソースからのメッセージを有効性証明するように依頼するために、ターミナルによって用いられる。メッセージは、暗号化され、かつチャレンジおよびレスポンスの２部分に分けてやって来る。

Validate Privateコマンドを受け取った際、ＢＩＡは、チャレンジメッセージのテキストを、「ＯＫ〈チャレンジ〉？」のようにＬＣＤ上に表示するが、ターミナルにはこれを送らない。個人がチャレンジを有効性証明したとき、レスポンスがＢＩＡによって秘密セッション鍵を用いて暗号化され、ＯＫレスポンスコードとともにターミナルに返される。個人がチャレンジの有効性証明をしなかったとき、ＢＩＡは、ＬＣＤスクリーンにも表示される「あなたのリクエストによりトランザクションをキャンセルしました」というテキストとともに、「失敗」レスポンスコードを返す。

ターミナルは、チャレンジまたはレスポンスの平文を見ることを許可されることは決してないことに注意せよ。

Reset

Resetコマンドは、ＢＩＡに、全ての一時的レジスタＬＣＤスクリーン、全ての一時的鍵レジスタをクリアし、点灯している可能性のある全てのキーパッドライトを消灯するように命令する。

Set ＰＩＣ〈値〉

このコマンドは、ＢＩＡのＰＩＣレジスタを〈値〉に割り当てる。安全にされていない(non-secured)装置がＰＩＣを提供することを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set Account index code〈値〉

このコマンドは、ＢＩＡのアカウントインデックスコードレジスタを〈値〉に割り当てる。安全にされていない装置がアカウントインデックスコードを提供す

ることを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set Title Index Code〈値〉

このコマンドは、ＢＩＡのタイトルインデックスコードレジスタを〈値〉に割り当てる。安全にされていない装置がタイトルインデックスコードを提供することを許すことは、セキュリティ問題になる可能性があることに注意せよ。なぜなら、安全にされていない装置は、盗聴または交換にあう危険性がずっと大きいからである。

Set金額〈値〉

このコマンドは、ＢＩＡの金額レジスタを〈値〉に割り当てる。

Decrypt Response〈暗号化されたレスポンスメッセージ〉

Decrypt Responseコマンドは、ＢＩＡに、その現在のレスポンス鍵を用いてレスポンスメッセージの暗号化された部分を復号化するように命令する。復号化がなされると、レスポンスは制御装置に返され、おそらくはＡＴＭターミナルのＬＥＤスクリーン上で表示される。

この復号能力を提供することはセキュリティ問題である。なぜなら、ターミナルは、平文がＢＩＡを離れると、それを用いてそれが行うであろうことを行う能力を有するからてある。

ＢＩＡソフトウェア：サポートライブラリ

ＢＩＡソフトウェアは、いくつかの異なるソフトウェアライブラリによってサポートされる。そのいくつかは標準的、一般に利用可能なライブラリであるが、またいくつかは、ＢＩＡに関して特別な要求事項を有するものである。

乱数発生器

ＢＩＡは、メッセージ本体およびメッセージレスポンス暗号化に使用するために、常にランダムなＤＥＳ鍵を選択しているため、選択された鍵が予測不可能な鍵であることが重要である。もし乱数発生器が１日の時刻あるいはその他の外部的に予測可能なメカニズムによっていると、暗号化鍵はそのアルゴリズムを知っ

ている敵による類推がずっと容易になってしまう。ＢＩＡで用いる暗号化技術のセキュリティを確実にするために、乱数発生器アルゴリズムと暗号化アルゴリズムの両方とも公知であると仮定する。

ＤＥＳ鍵を生成するための標準的な乱数発生アルゴリズムは、ＡＮＳＩ Ｘ９．１７、appendixＣ（当該技術において公知）中に定義されている。

ＤＳＰバイオメトリック符号化アルゴリズム

バイオメトリック符号化アルゴリズムは、人間の指先上の、うね(ridge)の終わりかたおよび分岐によって形成される詳細を探すための、専用の(proprietary)アルゴリズムである。詳細の完全なリストがＤＰＣ内にリファレンスとして格納されている一方、識別候補と登録された個人との間の比較を行う際には、部分的なリストのみしかアルゴリズムは要求しない。

バイオメトリック登録および識別の両方の際において、符号化アルゴリズムは、バイオメトリック入力ステップが終わるまでに十分な詳細が見つけられる(found)ことを確実にする。

オペレーティングシステムおよびデバイスドライバ

ＢＩＡはリアルタイム計算環境であり、そのため、それを実行するためのリアルタイム埋め込みオペレーティングシステムが必要である。オペレーティングシステムは、装置から割り込み(interrupt)をとり、タスクをスケジューリングする役目を果たす。

各デバイスドライバは、オペレーティングシステムと特定のハードウェアとの間のインターフェースの役割を果たす。例えばＰＩＣパッドデバイスドライバやＣＣＤスキャナデバイスドライバである。ハードウェアは、「ＰＩＣパッドキーが押された」や「ＣＣＤスキャナのスキャンが完了した」などのイベントの源である。デバイスドライバは、そのような割り込みを扱い、イベントを解釈し、イベントに対するアクションを行う。

ＤＥＳ暗号化ライブラリ

ＤＥＳのインプリメンテーションは公知のものがいくらでもある。ＤＥＳのイ

ンプリメンテーションは、５６ビットシークレット鍵を用いて、平文から暗号文(ciphertext)へのシークレット鍵型暗号化および、暗号文から平文への復号化を、提供する。

公開鍵暗号化ライブラリ

公開鍵暗号化サポートライブラリは、ＲＳＡ公開鍵特許（当該分野で公知）の所有者であるPublic Key Partnersから入手可能である。公開鍵暗号システム（Public Key cryptosystem）は、コストがかかるシークレット鍵の交換を必要とすることなしに通信することを可能にする、非対称暗号化システムである。公開鍵暗号化システムを使用するためには、公開鍵を用いてＤＥＳ鍵を暗号化し、次にＤＥＳ鍵を用いてメッセージを暗号化する。ＢＩＡは、公開鍵暗号システムを用いて、シークレット鍵の安全な交換を可能にする。

残念なことに、公開鍵システムはシークレット鍵システムよりもテストが非常に遅れており、そのためこの種のアルゴリズム全体に対する信頼レベルが低い。従って、本発明は、公開鍵暗号作成法を、通信セキュリティおよび短期信用情報交換(credential exchange)に用い、秘密(secrets)の長期保存には用いない。ネットワーククリデンシャルを作成するために、エンドユーザー個人および銀行の両方が、ＤＰＣによって識別される。ネットワーククリデンシャルは、エンドユーザー個人の識別ならびに、接続の文脈（すなわちＴＣＰ／ＩＰソースおよび行先ポート(destination port)）を包含する。

ＤＵＫＰＴ鍵管理ライブラリ

最初の鍵と、メッセージシーケンス番号が与えられれば、デライブドユニーク鍵／トランザクション（ＤＵＫＰＴ）管理を用いて、将来のＤＥＳ鍵を作成する。将来の鍵は、将来鍵テーブルに格納されている。ある鍵は、いったん使用されるとテーブルからクリアされる。最初の鍵は、最初の将来鍵テーブルを作成するためのみに用いられる。従って、最初の鍵はＢＩＡに格納されない。

ＤＵＫＰＴの使用は、最初の鍵を痕跡を残すことなく、各トランザクションに対して異なるＤＥＳ鍵を提供する鍵管理メカニズムを作成することを意図している。この意味するところは、もし将来鍵テーブルがうまく手に入れられて解体(d

issect)されたとしても、以前に送られたメッセージが曝露されることはないということであり、送信される情報の寿命が何十年にもなる場合には、これは非常に重要なゴールである。ＤＵＫＰＴは、ＡＮＳＩ Ｘ９．２４（当該分野において公知）に完全に規定されている。

ＤＵＫＰＴはもともと、デビットカード(debit card)トランザクション用の、ＰＩＣ暗号化メカニズムをサポートするために開発された。この環境においては、全てのトランザクションを保護することが重要であった。犯罪者が、６ヶ月間暗号化トランザクションを記録して、ＰＩＣパッドを手に入れそこから暗号化コードを抽出するのに成功したと仮定する。すると犯罪者は、その６ヶ月間の間に送信された各メッセージに対して、１つの新しい偽造デビットカードを製造することができる。しかしＤＵＫＰＴ下においては、犯罪者の窃盗および解体によって以前のメッセージが復号化されることはない（ただし犯罪者が解体後にＰＩＣパ

ッドを交換したとすれば新しいメッセージは依然として復号化可能である）

バイオメトリック－ＰＩＣ状況においては、犯罪者にとってより困難性が増す。なぜなら、メッセージが復号化されたとしても、デジタルバイオメトリック－ＰＩＣを肉体的な指紋に変換することは、アカウントナンバー－ＰＩＣをプラスチックカードに変換することよりもずっと困難であるためであり、これは、トークンレスシステムの大きな利点の１つである。

しかしながら、もし犯罪者が復号化することが可能であるならば、暗号化もできるわけであり、バイオメトリック－ＰＩＣをシステムに電子的に入力して詐欺的なトランザアクションを承認させることが可能かもしれない。これは非常に困難ではあるが、それでも犯罪者に利用可能なオプションはなるべく制限する方がよいため、ＤＵＫＰＴを使用する。

ＢＩＡソフトウエアコマンドセット

ＢＩＡソフトウエア：小売コマンドセット

ＢＩＡ／小売ソフトウエアインターフェースは、特定の小売ＰＯＳターミナルがシステムと相互作用することを許すインターフェースをエクスポートする。

ＢＩＡ／小売インターフェースは、ターミナルが次の動作を実行することを許すように設計されている。

取引承認

それらの動作を履行するために、ＢＩＡ／小売は、次のコマンドセットを供給する。

・Ｓｅｔ Ｌａｎｇｕａｇｅ〈言語ー名〉

・Ｇｅｔ Ｂｉｏｍｅｔｒｉｃ〈時間〉

・Ｇｅｔ ＰＩＣ〈時間〉

・Ａｓｓｉｇｎ Ｒｅｇｉｓｔｅｒ〈レジスタ〉〈値〉

・Ｇｅｔ Ａｃｃｏｕｎｔ ｉｎｄｅｘ ｃｏｄｅ〈時間〉

・Ｖａｌｉｄａｔｅ Ａｍｏｕｎｔ〈アマウント〉〈時間〉

・Ｅｎｔｅｒ Ａｍｏｕｎｔ〈時間〉

・Ｆｏｒｍ Ｍｅｓｓａｇｅ〈タイプ〉

・Ｓｈｏｗ Ｒｅｓｐｏｎｓｅ〈暗号化されたレスポンス〉〈時間〉

・Ｒｅｓｅｔ

ＢＩＡソフトウエア：ＣＡＴＶ（一体化されたリモート）コマンドセット

ＢＩＡ／ＣＡＴＶソフトウエアインターフェースは、電話／ＣＡＴＶＢＩＡと一体化されたターミナルがシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

遠隔取引承認

その動作を履行するために、ＢＩＡ/ＣＡＴＶは、次のコマンドセットを提供する。

・Ｇｅｔ Ｂｉｏｍｅｔｒｉｃ〈時間〉

・Ｓｅｔ ＰＩＣ〈テキスト〉

・Ａｓｓｉｇｎ Ｒｅｇｉｓｔｅｒ〈レジスタ〉〈テキスト〉

・Ｓｅｔ Ａｃｃｏｕｎｔ ｉｎｄｅｘ ｃｏｄｅ〈テキスト〉

・Ｆｏｒｍ Ｍｅｓｓａｇｅ〈タイプ〉

・Ｄｅｃｒｙｐｔ Ｒｅｓｐｏｎｓｅ〈暗号化されたレスポンスメッセージ〉

・Reset

ＢＩＡソフトウエア：一体化されたファクスコマンドセット

ＢＩＡ／ファクスソフトウエアインターフェースは、ファクスＢＩＡと一体化されたターミナルがシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

・安全ファクス提出（Secure Fax Submit）

・安全ファクスデータ（Secure Fax Data）

・安全ファクス追跡（Secure Fax Tracking）

・安全ファクス取り出し（Secure Fax Retrieve）

・安全ファクス拒否（Secure Fax Reject）

・安全ファクスアーカイブ（Secure Fax Archive）

・安全ファクス契約受諾（Secure Fax Contact Accept）

・安全ファクス契約拒否（Secure Fax Contact Reject）

・電子ドキュメントアーカイブ取り出し（Electronic Document Archive Retrieve）

これらの動作を履行するために、ＢＩＡ／ファクスは、次のコマンドセットを提供する。

・Get Biometric〈時間〉

・Set ＰＩＣ〈テキスト〉

・Set Title Index Code〈テキスト〉

・Assign Register〈レジスタ〉〈値〉

・Get Message Key

・Form Message〈タイプ〉

・Decrypt Response〈暗号化されたレスポンスメッセージ〉

・Reset

ＢＩＡソフトウエア：登録コマンドセット

ＢＩＡ／Regインターフェースは、汎用コンピュータが個人を識別し登録するようにシステムと相互作用することを許すインターフェースをエクスポートする

。次の動作がサポートされる。

個人の識別

バイオメトリック登録

それらの動作をサポートするために、ＢＩＡ/Regは、次のコマンドセットを提供する。

・Set Language〈言語ー名〉

・Get Biometric〈時間〉［プライマリ｜セカンダリ］

・Get ＰＩＣ〈時間〉

・Assign Register〈レジスタ〉〈テキスト〉

・Get Message Key

・Form Message〈タイプ〉

・Show Response〈暗号化されたレスポンス〉〈時間〉

・Reset

ＢＩＡソフトウエア：ＰＣコマンドセット

ＢＩＡ／ＰＣソフトウエアインターフェースは、汎用コンピュータが電子ドキュメントを送り、受信し、電子ドキュメントに署名し、ネットワークにわたって取引きを指揮し、ネットワーク上のサイトへのバイオメトリックー導出（biometric-derived）クレデンシャルを提供することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

・電子ドキュメント提出（Electronic Document Submit）

・電子ドキュメントデータ（Electronic Document Data）

・電子ドキュメント追跡（Electronic Document Tracking）

・電子ドキュメント取り出し（Electronic Document Retrieve）

・電子ドキュメント拒否（Electronic Document Reject）

・電子ドキュメントアーカイブ（Electronic Document Archive）

・電子ドキュメントアーカイブ取り出し（Electronic Document Archive Retrieve）

・電子署名サブミッション（Electronic Signature Submission）

・電子署名チェック（Ｅlectronic Ｓignature Ｃheck）

・遠隔取引承認（Ｒemote Ｔransaction Ａuthorization）

・ネットワーククレデンシャル（Ｎetwork Ｃredential）

・保護された接続（Ｓecured Ｃonnection）

これらの動作をサポートするために、ＢＩＡ／ＰＣは、次のコマンドセットを提供する。

・Ｓet Ｌanguage〈言語－名〉

・Ｇet Ｂiometric〈時間〉

・Ｇet ＰＩＣ〈時間〉

・Ｇet Ａccount index code〈時間〉

・Ｖalidate Ａmount〈アマウント〉〈時間〉

・Ｅnter Ａmount〈時間〉

・Ｖalidate Ｄocument〈名〉〈時間〉

・Ａssign Ｒegister〈レジスタ〉〈テキスト〉

・Ｇet Ｍessage Ｋey

・Ｆorm Ｍessage〈タイプ〉

・Ｓhow Ｒesponse〈暗号化された応答〉〈時間〉

・Ｖalidate Ｐrivate〈暗号化された有効性証明〉〈時間〉

・Ｒeset

ＢＩＡソフトウエア：発行者コマンドセット

ＢＩＡ／Ｉssソフトウエアインターフェースは、汎用コンピュータがバッチ変更リクエストを認証し提出するようにシステムと相互作用することを許すインターフェースをエクスポートする。次の動作がサポートされる。

発行者バッチ

この動作を履行するために、ＢＩＡ／Ｉssは、次のコマンドセットを提供する。

・Ｓet Ｌanguage〈言語－名〉

・Ｇet Ｂiometric〈時間〉［プライマリ｜セカンダリ］

・Ｇｅｔ　ＰＩＣ〈時間〉

・Ａｓｓｉｇｎ　Ｒｅｇｉｓｔｅｒ〈レジスタ〉〈値〉

・Ｇｅｔ　Ｍｅｓｓａｇｅ　Ｋｅｙ

・Ｆｏｒｍ　Ｍｅｓｓａｇｅ〈タイプ〉

・Ｓｈｏｗ　Ｒｅｓｐｏｎｓｅ〈暗号化されたレスポンス〉〈時間〉

・Ｒｅｓｅｔ

ＢＩＡソフトウエア：内部コマンドセット

ＢＩＡ／Ｉｎｔは、汎用コンピュータが個人を識別するようにシステムと相互作用することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

個人の識別

この動作を履行するために、ＢＩＡ／Ｉｎｔは、次のコマンドセットを提供する。

・Ｓｅｔ　Ｌａｎｇｕａｇｅ〈言語－名〉

・Ｇｅｔ　Ｂｉｏｍｅｔｒｉｃ〈時間〉

・Ｇｅｔ　ＰＩＣ〈時間〉

・Ａｓｓｉｇｎ　Ｒｅｇｉｓｔｅｒ〈レジスタ〉〈値〉

・Ｇｅｔ　Ｍｅｓｓａｇｅ　Ｋｅｙ

・Ｆｏｒｍ　Ｍｅｓｓａｇｅ〈タイプ〉

・Ｓｈｏｗ　Ｒｅｓｐｏｎｓｅ〈暗号化されたレスポンス〉〈時間〉

・Ｒｅｓｅｔ

ＢＩＡソフトウエア：ＡＴＭコマンドセット

ＢＩＡ／ＡＴＭソフトウエアインターフェースは、ＡＴＭが個人を識別（identify）することを許すコマンドセットをエクスポートする。次の動作がサポートされる。

アカウントアクセス

この動作を履行するために、ＢＩＡ／ＡＴＭは次のコマンドセットを提供する。

・Ｇｅｔ Ｂｉｏｍｅｔｒｉｃ〈時間〉

・Ｓｅｔ ＰＩＣ〈テキスト〉

・Ｓｅｔ Ａｃｃｏｕｎｔ ｉｎｄｅｘ ｃｏｄｅ〈テキスト〉

・Ａｓｓｉｇｎ Ｒｅｇｉｓｔｅｒ〈レジスタ〉〈値〉

・Ｆｏｒｍ Ｍｅｓｓａｇｅ〈タイプ〉

・Ｄｅｃｒｙｐｔ Ｒｅｓｐｏｎｓｅ〈暗号化されたレスポンスメッセージ〉

・Ｒｅｓｅｔ

ターミナル

ターミナルは、ＢＩＡを制御し、モデム、Ｘ.25接続、またはインターネット接続（業界において公知の方法）を介してＤＰＣと接続する装置である。ターミナルは、異なる形状および大きさを有し、タスクを実行するために異なるバージョンのＢＩＡを必要する。バイオメトリック入力装置にコマンドを発行、およびそこから答を受け取る電子装置はいずれもターミナルであり得る。

一部のターミナルは、汎用マイクロコンピュータ上でランされるアプリケーションプログラムであり、他のターミナルは、特定目的ハードウェアおよびソフトウェアのコンビネーションである。

ターミナルが、全体的にシステムの機能にとって決定的に重要である一方で、システム自体はターミナルに少しも信頼をおいていない。ターミナルがシステムに情報を提供する度に、確認のための個人への提示、または他の予め登録された情報とのクロスチェックによって、システムは常に何らかの手法によりそれを確認する。

ターミナルが、データがＢＩＡに適切に処理されたことを確認するためにＢＩＡメッセージの一部を読みとることが可能な一方で、ターミナルはバイオメトリック、ＰＩＣ、暗号化鍵、またはアカウントインデックスコードを含むバイオメトリック識別情報を読みとることはできない。

特定のＢＩＡは、ＰＩＣエントリ、および秘密コードディスプレイなど何らかのセキュリティ機能をターミナルにエクスポートする。その結果、そのような装置は、完全に内蔵された同一のもの(their entirely self-contained counterpa

rts)と比べて安全性が低いとみなされ、そのため結果的に低いセキュリティ評点を有することになる。

多くの異なるターミナルのタイプがあり、それぞれは特定のモデルＢＩＡに接続される。それぞれのターミナルを、以下に簡単に説明する。

ＡＴＭ(Automated Teller Machinery)

ＡＴＭソフトウェアのロードを伴う一体型ＢＩＡ/ＡＴＭは、ＡＴＭキャッシュディスペンサへのバイオメトリック-ＰＩＣのアクセスを提供する。

ＢＲＴ(Biometric Registration Terminal)

マイクロコンピュータに付属するレジスタレーションソフトウェアのロードを伴う標準ＢＩＡは、銀行に、財政アカウント評価および他の個人情報とともに新規の個人のシステムへの登録を可能にする。

ＣＥＴ(Certified Email Terminal)

マイクロコンピュータに付属するＰＣソフトウェアのロードを伴う標準ＢＩＡは、個人が、認証された電子メールメッセージを送信、受信、アーカイブ化、拒否、およびトラックすることを可能にする。

ＣＰＴ(Cable-TV Point of Sale Terminal)

ＣＡＴＶ広帯域に付属するＣＡＴＶソフトウェアのロードを伴うＢＩＡ/ｃａｔｖは、バイオメトリック-テレビ(または「ＴＶ」)リモコンを有する個人が、テレビショッピングでの購入を承認することを可能にする。

ＣＳＴ(Customer Service Terminal)

マイクロコンピュータシステムに付属するインターナルソフトウェアのロードを伴う標準ＢＩＡは、従業員が顧客サービスの目的でデータベースリクエストを構築することを承認する。

ＥＳＴ(Electronic Signature Terminal)

マイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準ＢＩＡは、個人が、書類への電子署名を構築し検証することを可能にする。

ＩＰＴ(Internet Point of Sale Terminal)

マイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準ＢＩＡは、インターネット接続を有する個人が、インターネットに接続したマーチャントから製品を購入することを可能にする。

ＩＴ(Issuer Terminal)

マイクロコンピュータに付属する発行者ソフトウェアのロードを伴う標準ＢＩＡは、銀行が、資産アカウントのバッチされた変更をＤＰＣへ送信することを可能にする。

ＩＴＴ(Internet Teller Terminal)

インターネット接続を有するマイクロコンピュータに付属するパーソナルコンピュータソフトウェアのロードを伴う標準ＢＩＡは、個人が、所望のインターネット銀行とのトランザクションを行うことを可能にする。

ＰＰＴ(Phone Point of Sale Terminal)

電話と一体化されたＣＡＴＶソフトウェアのロードを伴うＢＩＡ/ｃａｔｖは、個人が、電話でのトランザクションを承認することを可能にする。

ＲＰＴ(Retail Point of Sale Terminal)

X.25ネットワークに付属するまたはモデムを使用するリテイルソフトウェアのロードを伴う標準ＢＩＡは、個人が店においてトランザクション承認を使用してアイテムを購入することを許可する。

ＳＦＴ(Secure Fax Terminal)

ファックスマシンと一体化されたファックスソフトウェアのロードを伴うＢＩＡ/ｃａｔｖは、個人が、安全なファックスメッセージを送信、受信、拒否、アーカイブ化、およびトラックすることを可能にする。

ターミナル：小売りPOSターミナル

RPTの目的は、個人が現金、小切手、デビットカードまたはクレジットカードのいずれをも用いる必要なく店舗で品物を購入することを可能にすることである。

RPTは、個人からマーチャントへの金銭的トランザクションを承認するためにBIA／小売りを用いる。RPTは、バイオメトリック－PIC承認を受け入れるために用

いられることに加えて、標準のデビットカードおよびクレジットカード走査機能をも提供する。

RPTはまた、オプションのスマートカードリーダだけでなく、標準のクレジットおよびデビット磁気ストライプカードリーダをも含むと考えられる。

各RPTは、モデム、X.25ネットワーク接続、ISDN接続、または同様のメカニズムによりDPCに接続される。RPTはまた、トランザクションの量およびマーチャントコードが得られる電子キャッシュレジスタなどの他のデバイスにも接続され得る。

RPTの構成：

・BIA／小売り
・低価格のマイクロプロセッサ
・9.6kbモデム／X.25ネットワークインターフェースハードウェア
・不揮発性RAM内のマーチャント識別子コードナンバ
・BIAに接続されるDTCシリアルポート
・磁気ストライプカードリーダ（当該分野で公知である）
・ECR（電子キャッシュレジスタ）接続ポート
・オプションのスマードカードリーダ（当該分野で公知である）

DPCがBIAトランザクション承認要求に対して肯定的に応答するためには２つのエンティティ、すなわち、個人とマーチャントとが識別される必要がある。

個人はバイオメトリック－PICにより識別され、マーチャントはDPCにより識別される。DPCは、BIAのVAD記録内に含まれるマーチャントコードを、RPTによりトランザクション要求に追加されたマーチャントコードとクロスチェックする。

まず、マーチャントがトランザクションの値を電子キャッシュレジスタにエンタする。次いで、個人がバイオメトリック－PICおよびアカウントインデックスコードをエンタし、その後量を確認する。RPTはその後、製品情報とマーチャントコードとをBIAに追加し、トランザクションを作成するようにBIAに指示し、そしてネットワーク接続（モデム、X.25など）を介してトランザクションをDPCに送信する。

DPCは、このメッセージを受け取ると、バイオメトリック－PICの有効性を証明し、インデックスコードを用いてアカウントナンバを獲得し、メッセージ内のマーチャントコードを、BIAの登録されたオーナとクロスチェックする。すべてが合致した場合、DPCは交換を実行するためにクレジット／デビットトランザクションを形成して送信する。クレジット／デビットネットワークからのレスポンスは、秘密コードに追加されてトランザクションレスポンスメッセージを形成する。DPCはその後、トランザクションレスポンスメッセージをRPTに送り返す。RPTは、承認が成功したか否かを見るためにレスポンスを調べ、その後レスポンスをBIAにフォワードする。するとBIAは、個人の秘密コードを表示して、トランザクションを終了する。

RPTとDPCとの間のメッセージは、暗号化およびBIAからのMAC演算によって安全化される。MACは、RPTがメッセージの暗号化されていない部分を調べることを可能にするが、RPTは上記部分を変更することができない。暗号化は、メッセージの暗号化された部分がRPTに開示されることを妨げる。

各小売りBIAは、マーチャントに登録されなければならない。このことは、BIA窃盗を思いとどまらせることを補助する。さらに、RPTは各メッセージにマーチャントコードを追加するため、マーチャントのBIAが異なるBIAで置換されると、DPCで行われるクロスチェックにより検出される。

ターミナル：インターネットPOS

インターネットPOS(IPT)の目的は、コンピュータを使用している個人からマーチャントへのクレジットおよびデビットの金銭的トランザクションを承認することである。この場合、個人およびマーチャントの両方がインターネット上にいる。

インターネットは、単に、マーチャント、DPC、およびIPTのすべてがリアルタイムで互いに接続できる汎用ネットワークを表すにすぎないことに留意されたい。その結果、このメカニズムは、他のいずれの汎用ネットワークとも全く同様に作用する。

IPTの構成：

・BIA／PC

・マイクロコンピュータ

・インターネットショッパソフトウェアアプリケーション

・インターネット（または他のネットワーク）接続

IPTは、個人を識別することに加えて、トランザクションの相手である遠隔のマーチャントをも識別しなければならない。マーチャントはまた、DPCとIPTの両方を識別しなければならない。

インターネットショッパプログラムは、購入が行われているマーチャントのホストネーム（または他の形態のネットネーム）を、マーチャントが誰であるかを検証するために格納する。マーチャントはすべての合法なインターネットホストをDPCに登録しているため、このことは、DPCがマーチャントコードを、ホストネームで格納されているマーチャントコードとクロスチェックしてマーチャントが誰であるかを検証することを可能にする。

まず、IPTは、インターネットを用いてマーチャントに接続する。一旦接続が確立されると、IPTはセッション鍵を生成してマーチャントに送信することにより、接続を安全化する。セッション鍵が開示されないように保護されていることを保証するために、セッション鍵は、公開鍵暗号化を用いてマーチャントの公開鍵で暗号化される。マーチャントは、暗号化されたセッション鍵を受け取ると、秘密鍵を用いてそれを復号化する。このプロセスを、公開鍵暗号化シークレット鍵交換を介して接続を安全化するという。

一旦接続されると、IPTは、マーチャントからマーチャントコード、および価格と製品との両方の情報をダウンロードする。一旦個人が購入を行う準備ができると、個人は購入したい商品を選択する。その後、個人は、BIA／PCを用いてバイオメトリック－PICをエンタする。IPTはマーチャントコード、製品識別情報、および量をBIAに送信し、遠隔トランザクション承認要求を作成するようにBIAに指示する。その後、IPTは安全なチャネルを介して要求をマーチャントに送信する。

マーチャントは、IPTがマーチャントと有するものと同一の種類の安全な接続

を介して、すなわち、公開鍵暗号化を用いて、DPCに接続して安全なセッション鍵を送信する。しかし、IPT－マーチャント接続とは異なり、マーチャント－DPCセッション鍵は、１接続だけでなく１日中有効である。

マーチャントはDPCに接続して、セッション鍵を用いて接続を安全化し、有効性証明のためにトランザクションをDPCにフォワードする。DPCは、バイオメトリック－PICの有効性を証明し、要求に含まれるマーチャントコードを要求内で送信されたホストネームで格納されているマーチャントコードとクロスチェックし、その後トランザクションをクレジット／デビットネットワークに送信する。一旦クレジット／デビットネットワークが応答すると、DPCは、クレジット／デビットの承認、暗号化された秘密コード、および個人のアドレスを含む応答メッセージを作成して、そのメッセージをマーチャントに送り返す。

マーチャントは一旦応答を受け取ると、応答から個人のメーリングアドレスをコピーして、承認コードを記録し、IPTに応答メッセージをフォワードする。

IPTはBIAへの応答を取り扱い、BIAは秘密コードを復号化してLCDスクリーン上に表示し、DPCが個人を認識したことを示す。IPTはまた、成功したか失敗であったかにかかわらず、トランザクションの結果を示す。

システムは概して、ネットワーク上の敵はいずれの点においてもネットワーク接続をハイジャックすることが可能であると仮定しているため、すべてのパーティはリアルタイムインタラクション中に安全な通信を有していなければならない。主な懸念は、情報の開示ではなく、メッセージの挿入または再送信である。

公開鍵暗号化のシステム全体が公開鍵用の信頼されたソースを有することに依存している。これらの信頼されたソースは、証明オーソリティと呼ばれており、このようなソースが近い将来インターネット上で使用可能であると考える。

ターミナル：インターネットテラーターミナル

インターネットテラーターミナル（ＩＴＴ）は、インターネット銀行トランザクションセッションの際に個人を識別するために利用される。ＤＰＣ、銀行のコンピュータシステム、および個人は全てインターネットに接続している。

２つの主要タスクがある。第１の主要タスクは、ＩＴＴからインターネット銀

行への安全な通信チャネルを提供することである。第２の主要タスクは、インターネット銀行に完璧な識別証明書を提供することである。この両方が達成されればすぐに、ＩＴＴは、安全なインターネット銀行トランザクションセッションを提供することができる。さらに、ＢＩＡの課題である応答検証能力は、全ての高額および/またはイレギュラーなトランザクションに対してさらなる安全性を提供するために使用される。

ＩＴＴは、以下から構成される、すなわち

・ＢＩＡ(標準ＰＣモデル)

・マイクロコンピュータ

・インターネットテラー（Internet Teller）ソフトウェアアプリケーション

・インターネット接続

ＩＴＴは、個人のインターネットターミナルとして機能するマイクロコンピュータに接続されたＢＩＡ／ＰＣを用いて、バイオメトリック識別を承認する。

個人および銀行の両方か、ＤＰＣによって識別され、それによって、ネットワーククリデンシャルが作成される。ネットワーククリデンシャルは、個人の識別および接続の内容（すなわち、ＴＣＰ／ＩＰソースおよびデスティネーションポート）を含む。

ＤＰＣは、ＩＴＴがＤＰＣに送る銀行のホストネームと、銀行がＩＴＴに送るコードとをクロスチェックすることにより銀行を識別する。

第１に、ＩＴＴはインターネット銀行に接続し、銀行が、個人のための新しいセッションを扱うために必要とされるコンピューティングリソースを有することを確認する。銀行が十分なリソースを有する場合、銀行識別コードをＩＴＴに送り返す。

一旦接続されれば、ＩＴＴは、バイオメトリックＰＩＣおよびアカウントインデックスコードを個人から入手することをＢＩＡに指示する。次にＩＴＴは、銀行のホストネームおよび銀行コードの両方を加える。この情報の全てを用いて、ＢＩＡは、次に、インターネットを介してＩＴＴがＤＰＣに送るネットワーククリデンシャルリクエストメッセージを作成するように依頼される。

ＤＰＣがこのメッセージを受け取れば、ＤＰＣは、バイオメトリックＰＩＣの有効性を証明し、インデックスコードを用いてアカウントナンバーを入手し、メッセージからの銀行コードが、遠隔マーチャントデータベースにおける銀行のホストネームの下に格納された銀行コードと一致するかどうかを確認する。ＤＰＣはまた、インデックスコードによって返されたアカウントナンバーが、銀行のものであるかの確認を行うためにチェックする。すべてがチェックされれば、次に、ＤＰＣは、個人のアカウント識別、その日の時間、および銀行コードを用いてネットワーククリデンシャルを作成する。ＤＰＣは、公開鍵暗号化およびＤＰＣの秘密鍵を用いて、このクリデンシャルに署名する。ＤＰＣは、銀行の公開鍵および個人の秘密コードを取り出し、そしてクリデンシャルを用いてネットワーククリデンシャルレスポンスメッセージを形成する。レスポンスメッセージは、ＢＩＡレスポンス鍵を用いて暗号化され、その後、ＩＴＴに送り返される。

ＩＴＴがそのレスポンスを受け取る時、ＩＴＴは、ＢＩＡにレスポンスメッセージを渡す。ＢＩＡは、復号化を行い、次に、個人の秘密コードをＬＣＤスクリーン上に表示する。銀行の公開鍵は、公開鍵レジスタに格納される。２つのランダムセッション鍵は、ＢＩＡによって生成される。共用セッション鍵と呼ばれる第１の鍵は、平文でＩＴＴに明らかにされる。ＩＴＴは、この共用セッション鍵を用いることにより、銀行との接続を確実にする。

秘密セッション鍵と呼ばれる他方のセッション鍵は、ＩＴＴと共用されない。これは、ＢＩＡのチャレンジ－レスポンスメカニズムのために用いられ、このメカニズムは、銀行が、（信用できない）ＩＴＴに関与することなしに、個人から直接の非ルーチントランザクションに対する特定の有効性の証明を得ることを可能する。

共用セッション鍵を受け取った後、ＩＴＴは、ＢＩＡに、セッション鍵とネットワーククリデンシャルの両方を含み、銀行の公開鍵を用いて全て暗号化される安全接続要求メッセージを作成するように依頼する。ＩＴＴは次に、安全接続要求メッセージを銀行に送る。

銀行は、リクエストメッセージを受け取ると、銀行自身の秘密鍵を用いてメッ

セージを復号化する。その後、ＤＰＣの公開鍵を用いて実際のネットワーククリデンシャルを復号化する。ネットワーククリデンシャルが有効で、期限が切れていなければ（クリデンシャルは、ある数分後に時間切れとなる）、その個人は承認され、安全を確実にするために使用されるセッション鍵を用いて、会話が継続する。

個人が、非ルーチンまたは高価値のトランザクションを行う場合、銀行は、さらなる安全のために個人がこれらのトランザクションの有効性の証明をすることを求めることを所望し得る。そうするためには、銀行は、秘密セッション鍵を用いて暗号化されたチャレンジーレスポンスメッセージをＩＴＴに送り、ＩＴＴは、そのチャレンジーレスポンスメッセージをＢＩＡにフォワードする。ＢＩＡは、メッセージを復号化し、チャレンジ（通常、「$2031.23をリック・アダムスに振替ＯＫ？」の形態）を表示し、個人がＯＫボタンを打つことにより有効性の証明をすれば、ＢＩＡは秘密セッション鍵を用いてレスポンスを再び暗号化し、そのメッセージをＩＴＴに送り、ＩＴＴは、そのメッセージを銀行にフォワードし、トランザクションの有効性を証明する。

このシステムは、クリデンシャルを提供し、かつＩＴＴと銀行との間の通信を確実とするために公開鍵暗号系を利用する。

このメカニズムが正しく機能するためには、銀行はＤＰＣの公開鍵を知っていなければならず、ＤＰＣは、銀行の公開鍵を知っていなければならない。システムの安全のためには、両方のパーティが、承認されていない改変から、互いの公開鍵を安全に管理することが重要である。公開鍵は、誰によっても読むことが可能であるが、ただ、誰によっても改変可能となることはできないことに注意されたい。もちろん、どのようなセッションまたは秘密鍵は、観察から安全に管理されなければならず、これらの秘密鍵は、セッションの終了後に破壊されなければならない。

非ルーチントランザクションのための余分な確認ステップは、ウイルス、ハッカー、および個人の無知が原因で、インターネット上でパーソナルコンピュータアプリケーションを保護することが比較的困難であるので、必要である。銀行は

、ユーティリティ会社、主なクレジットカードのベンダーなどのよく知られた機関への金銭振替のみを包含するように、ＩＴＴに利用可能なルーチン金銭振替をおそらく限定すべきである。

ターミナル：電子署名

電子署名ターミナル（ＥＳＴ）は、電子文書に関して偽造不可能である電子署名を作成するために個人によって使用される。ＥＳＴにより、個人が電子文書に署名すること、または、そのような文書にすでにある電子署名を検証することが可能となる。

ＥＳＴの構成：

・ＢＩＡ／ＰＣ

・マイクロコンピュータ

・メッセージダイジェストエンコーダアルゴリズム

・モデム、Ｘ．２５接続、またはインターネット接続

・電子署名ソフトウェアアプリケーション

ＥＳＴは、電子署名ソフトウェアアプリケーションによって制御されたイベントに関して、マイクロコンピュータに取り付けられたＢＩＡ／ＰＣを使用する。

ある種の公開／秘密鍵をかけられたトークンを使用することなしにデジタル署名を作成するためには、３つの事が行われなければならない。第１に、署名される文書は、固有に識別されなければならず、その日の時刻が記録されなければならず、署名を行っている個人が識別されなければならない。これにより、文書、個人、および時刻がリンクされ、一意のタイムスタンプされた電子署名が作成される。

第１に、署名される文書は、メッセージダイジェストコードを生成するメッセージダイジェストコード化アルゴリズムによって処理される。このようなアルゴリズムの１つに、当該分野でよく知られている、ＲＳＡによるＭＤ５アルゴリズムがある。本来、メッセージダイジェストアルゴリズムは、同じメッセージダイジェストコードを生成する別の文書を提示することがほとんど不可能となるように特別に設計されている。

次に、個人は、ＢＩＡを用いてバイオメトリックＰＩＣを入力し、メッセージダイジェストコードはＢＩＡに渡され、文書名が加えられ、その結果生じるデジタル署名リクエストメッセージが、識別および保存のためにＤＰＣに送られる。

ＤＰＣはリクエストを受け取り、バイオメトリック識別チェックを行い、個人が一旦検証されれば、メッセージダイジェストコード化と、個人のバイオメトリックアカウントナンバーと、その日のその時の時刻と、文書名と、署名を集めたＢＩＡの識別を収集し、それら全てを電子署名データベース（ＥＳＤ）に格納する。ＤＰＣはその後、ＥＳＤレコードナンバー、日付、時刻、および署名者の名前から成る署名コードテキストストリングを作成し、この署名コードを個人の秘密コードと共に、ＥＳＴに送り返す。

電子署名をチェックするために、文書は、ＭＤ５アルゴリズム（当該分野で公知）を通して送られ、その結果生じる値は、電子署名コードと一緒に、ＢＩＡおよびリクエストしている個人のバイオメトリックＰＩＣに与えられ、メッセージはＤＰＣに送られる。ＤＰＣは、各署名の有効性チェックを行い、適切に応答する。

ＢＩＡは、電子署名に関係するどのようなデータも暗号化しないので、特定のＭＤ５の値と共に、文書タイトルが、平文で送られる。署名の有効性の証明に対しても、同じ状況が当てはまる。

従って、署名が偽造され得ない一方で、詳細のいくつか（文書名を含む）は、妨害に弱い。

ターミナル：証明された電子メールターミナル

証明電子メールターミナル（ＣＥＴ）の目的は、個人に、送り手の識別、受け取りおよび受け手両方の検証を提供し、メッセージ配送の秘密性を確実としながら、電子メッセージをシステム内の他の個人に送る方法を提供することである。

ＣＥＴは、ＢＩＡ／ＰＣを用いることにより、送り手および受け手の両方を識別する。安全は、メッセージを暗号化し、その後、アップロードの間に、送り手のＢＩＡを用いてメッセージ鍵を暗号化し、次に、ダウンロードの間に、受け手のＢＩＡを用いてメッセージ鍵を復号化する。

送信者および受け手のＣＥＴの構成：

・ＢＩＡ

・マイクロコンピューター

・モデム、Ｘ．２５接続、またはインターネット接続

・電子メールを受け取る能力

・証明された電子メールアプリケーション

実際、ＣＥＴは、電子メールアプリケーションと、証明された電子メールを送信および受信するためのバイオメトリックＰＩＣ承認を生じさせるためにＢＩＡを呼び出すネットワーク接続とを有するマイクロコンピュータである。

メッセージの配送を保証するために、送り手および受け手は共に、識別されなければならない。

送り手は、メッセージをＤＰＣにアップロードするときに、バイオメトリックＰＩＣを用いて、自分自身を識別する。送り手が文書を送ることを望む各受け手は、バイオメトリックアカウント識別ナンバーまたはファックス番号のどちらか一方、およびエクステンションによって識別される。受け手が、メッセージをダウンロードするためには、自分のバイオメトリックＰＩＣを用いて自分自身を識別する。この手順は、指名電話に似ている。

メッセージの配送は、個人が、文書またはメッセージをアップロードし、バイオメトリックＰＩＣを用いて自分自身を識別することで始まる。個人は、その後、文書名を検証し、電子メールメッセージは、暗号化され、アップロードされる。

メッセージが一旦アップロードされれば、送り手は、各受け手に対する文書の現在の配送ステータスをリクエストするために使用され得るメッセージ識別コードを受け取る。

ＤＰＣは、電子メールメッセージを各受け手に送り、証明されたメッセージが到着した時に、受け手に知らせる。

一旦受け手が告知を受け取れば、受け手は、都合のよい時に、バイオメトリックＰＩＣを入手し、ＤＰＣに有効性の証明をさせることにより、メッセージまた

はメッセージ群を受けるまたは拒否することのどちらかを選択し得る。

一旦、全ての受け手にうまく送信されれば、所定の期間後、通常２４時間後、文書は取り除かれる。文書を、メッセージが送られた全ての個人の表示と共にアーカイブ化することを望む個人は、メッセージの削除の前に、メッセージアーカイブリクエストを入力し得る。

送信の安全な面をもたらすために、文書は、途中で公開されることから保護される。ＣＥＴは、ＢＩＡによって生成される５６ビットメッセージ鍵を用いることにより、これを達成する。ＢＩＡは、バイオメトリックＰＩＣの一部としてメッセージ鍵を暗号化する責任を引き受けるので、暗号化鍵は、安全にＤＰＣに送られる。

個人がメッセージをダウンロードする時に、メッセージ鍵は、秘密コードとともに暗号化されて送られることにより、受け手がメッセージを復号化することが可能となる。全員が同じメッセージを受け取るので、全ての受け手がこのメッセージ鍵を持つようにしてもよいことに注目されたい。

ＩＴＴの場合と同じように、一旦個人が文書名の有効性を証明すれば、改変されたＣＥＴが所望のどのような文書も送ることができるので、個人は、ＣＥＴアプリケーションソフトウェアを不正な改変から保護するように注意しなければならない。

ターミナル：安全ファックスターミナル

安全ファックスターミナル（ＳＦＴ）の目的は、個人に、送り手の識別、受け取りおよび受け手両方の検証を提供し、メッセージ配送の秘密性を確実としながら、ファックスメッセージをシステム内の他の個人に配送する方法を提供することである。

各ＳＦＴは、送り手および受け手の両方を識別するために、集積型ＢＩＡ／ケーブルテレビを使用する。通信セキュリティは、暗号化を通して達成される。

送信者および受け手両方のＳＦＴの構成：

・ＢＩＡ／ケーブルテレビ

・ファックスマシン

・オプショナルのＩＳＤＮモデム

ＳＦＴは、モデムを介してＤＰＣに接続されたファックスマシンである。このシステムは、ファクスを、証明された電子メールの単なる別のタイプのものとして扱う。

安全なファックスに関して、セキュリティのいくつかの異なるレベルが存在するが、最も安全なバージョンにおいては、送り手および全ての受け手の身元が検証される。

送り手は、メッセージをＤＰＣに送る際に、バイオメトリックＰＩＣおよびタイトルインデックスコードを用いて、自分自身を識別する。ファックスを受け取るためには、リストされた各受け手が、バイオメトリックＰＩＣおよびタイトルインデックスコードを再び用いて自分自身を識別する。

さらに、受け取りサイトは電話番号によって識別される。この電話番号は、ＤＰＣを用いて登録される。安全な秘密のファックスに関しては、各受け手が、電話番号およびエクステンションを用いて識別される。

ＳＦＴが送ることのできるファクスには５つの基本的なタイプがある。

Ｉ．非安全性ファックス

安全にされていないファックスは、標準のファックスに等しい。送り手は、受け手のサイトの電話番号を入力し、ファックスを送る。この場合、送り手は、識別されないままで、ファックスは、正しい受け手に配送されることを期待して、与えられた電話番号に送られる。ＳＦＴは、そのような全ての安全にされていないファックスのトップラインに、「非安全性」（「UNSECURED」）であると目立つように印をつける。非ＳＦＴファックスマシンから受け取られた全てのファックスは、常に、非安全性であると印がつけられている。

ＩＩ．送り手安全ファックス

送り手安全ファックスにおいては、送り手は、ファックスマシンの「送り手安全」モードを選択し、タイトルインデックスコードに続いてバイオメトリックＰＩＣを入力する。次に、ファックスマシンは、ＤＰＣに接続し、バイオメトリックＰＩＣ情報を送る。一旦ＤＰＣが個人の同一性を検証すれば、個人は次に文書

をファックススキャナに送り込むことによりファックスを送る。この場合、ファックスは、実際に、ファックスをデジタル形式で格納するＤＰＣに送られる。一旦全部のファックスがＤＰＣに到着すれば、ＤＰＣは、各宛先にファックスを送ることを開始し、各ページは、各ページのトップに「送り手安全」（「SENDER-SECURED」）の大見出しとともに、名前、タイトル、および送り手の会社をラベル表示する。

ＩＩＩ．安全ファックス

安全ファックスにおいては、送り手は、ファックスマシンの「安全」モードを選択し、タイトルインデックスコードに続いてバイオメトリックＰＩＣを入力し、その後、受け手の電話番号を入力する。一旦システムが送り手の身元および各受け手の電話番号を検証すれば、その後、個人は、文書をファックススキャナに送り込むことによりファックスを送る。次に、ファックスは、ファックスをデジタル形式に格納するＤＰＣに送られる。一旦全部のファックスがＤＰＣに届けば、ＤＰＣは、未完の安全ファックス、送り手のタイトルおよび身元、そして、トラッキングコードと共に待機中のページ数を示す小さなカバーページを宛先に送る。このトラッキングコードは、自動的に受け手のファックスマシンのメモリに入力される。

ファックスを取り出すためには、受け手の会社の従業員が、ファックスマシンの「ファックス取り出し」ボタンを選択し、トラッキングコードを用いることにより、未完のどのファックスを取り出すかを選択し、次に、バイオメトリックＰＩＣを入力し得る。ファックスが不要な場合は、個人は、「ファックス拒絶」ボタンを押し得るが、それでもやはり、そうするためには、システムに対して自分自身の識別を行わなければならない。一旦会社のメンバーとして有効性を証明されれば、次に、ファックスは受け手のファックスマシンにダウンロードされる。各ページは、各ページのトップに、送り手の身元およびタイトル情報と共に、

「安全」（「SECURED」）の文字を有する。

ＩＶ．安全性秘匿ファックス

安全性秘匿ファックスにおいては、送り手は、ファックスマシンの「安全性秘

匿」モードを選択し、タイトルおよびインデックスコードに続いてバイオメトリックＰＩＣを入力し、次に、各受け手の電話番号およびシステムエクステンションを入力する。一旦ＤＰＣが送り手の身元および各受け手の電話番号およびエクステンションを検証すれば、個人は次に、ファックススキャナに文書を送り込むことにより、ファックスを送る。ファックスは、ファックスをデジタル形式で格納するＤＰＣに送られる。一旦全部のファックスがＤＰＣに届けば、ＤＰＣは、未完の安全性秘匿ファックス、送り手のタイトルおよび身元、受け手のタイトルおよび身元、そして、トラッキングコードと共に、待機中のページ数を示す小さなカバーページを各宛先に送る。このトラッキングコードは、自動的に受け手のファックスのメモリに入力される。しかし、ファックスを取り出すことのできる唯一の個人は、エクステンションコードが示されている個人である。

この個人は、「ファックス取り出し」ボタンを選択し、取り出すべき未完のファックスを選択し、次にバイオメトリックＰＩＣを入力する。一旦受け手としての有効性を証明されれば、ファックスは、次に受け手のファックスマシンにダウンロードされる。各ページは、各ページのトップに、送り手のタイトルおよび身元情報と共に「安全性秘匿」（「SECURED-CONFIDENTIAL」）の文字を有する。

Ｖ．安全性秘匿契約ファックス

このファックスは、受け手に対するファックスの実際の配送に関しては、ファックスが、安全性秘匿の代わりに「契約」とタイトルを付けられることを除いては、安全性秘匿ファックスと同様に処理される。さらに、ＤＰＣは、自動的に契約ファックスをアーカイブ化する。どのような受け手も、契約ファックスの受け取りに続くＳＦＴによって、契約を受けるまたは拒絶し得る。従って、オプションで、ＤＰＣは電子書記の役割を果たす。

システムに送られ、その後、受け手にフォワードされるどのようなファックスも、送信ファックスマシンをタイアップすることなしに、いかなる数の受け手にも送られ得る。さらに、送られたいかなるファックスのトラッキングナンバーが、ファックスマシンのメモリに入力され、継続中のいかなるファックスのステータスレポートが、「ステータス」ボタンを選択し、その後、特定のファックス未

完トラッキングコードを選択することにより、送信マシンにおいて生成され得る。ＤＰＣは、各受け手に対する送信状態を詳述し、送信ファックスマシンに直ちに送られるレポートを発行する。

いかなる安全または安全性秘匿ファックスに関して、送り手または受け手の１人のどちらか一方が、今後の参考のために、ファックスを（誰がファックスを送り、誰がファックスを受け取ったかに関する詳細と共に）アーカイブ化するというオプションが存在する。このために、いかなる安全ファックスも、成功した配送の後、ある期間（すなわち２４時間）保持される。アーカイブトラッキングコードは、アーカイブのリクエストがあればいつでも個人に戻される。このアーカイブコードは、ファックスと、システムにアーカイブ化されたファックスステータスレポートとの取り出しに使用される。

アーカイブされたファックスは、ある期間（すなわち２４時間）の後、読み取り専用の二次記憶装置に配置される。アーカイブ化されたファックスを取り出すことは、人の介入を必要とし、遂行に２４時間までかかり得る。

ＳＦＴシステムは、受け手が送り手の身元を確かめるために懸命に働き、受け手が実際に文書の受け取りを了承したことを送り手が確かめるために、同じ様に懸命に働く。

送り手と受け手との間の通信の妨害に対して保護を行うために、ファックスターミナルは、ＢＩＡによって提供されるメッセージ鍵機能を用いてファックスを暗号化する。ＢＩＡは、バイオメトリックＰＩＣの１部としてメッセージ鍵を暗号化する責任を取るので、暗号化鍵は、安全にＤＰＣに送られる。

個人が、いかなるタイプの安全ファックスを受け取るときには、メッセージ鍵は、秘密コードとともに暗号化されて送られることにより、受け手がメッセージを復号化することが可能となる。全員が同じメッセージを受け取るので、全ての受け手がこのメッセージ鍵を有するようにしてもよいことに注目されたい。

ターミナル：バイオメトリック登録ターミナル

バイオメトリック登録ターミナル（ＢＲＴ）の目的は、バイオメトリックＰＩＣ、メーリングアドレス、秘密コード、電子メールアドレス、タイトルと電子メ

ッセージおよびファックスの送信および受信に用いられるタイトルインデックスコードのリスト、および、財政的資産アカウントおよびアクセスでき得るアカウントインデックスコードのリストを含む新しい個人の登録をすべて、バイオメトリックＰＩＣを用いて行うことである。

登録プロセスの目的は、情報の有効性が証明され得る責任機関の場所で、個人から個人情報を得ることである。これは、リテイル銀行店および企業の人事部を含むが、それらに限定されるものではない。参加している責任機関の各々は、登録を行うことを承認された従業員のグループによって使用される１つのＢＲＴを有する。各従業員は、登録された各個人に対して責任がある。

ＢＲＴの構成：

・マイクロコンピューター、およびスクリーン、キーボード、マウス

・ＢＩＡ／Ｒｅｇ

・９．６ｋｂモデム／Ｘ．２５ネットワーク接続（当該分野で公知）

・バイオメトリック登録ソフトウェアアプリケーション

ＢＲＴは、バイオメトリック入力に対して、取り付けられたＢＩＡ／Ｒｅｇを用い、９．６ｋｂモデムまたはＸ．２５ネットワーク接続（当該分野で公知）によってシステムに接続される。バイオメトリック登録ターミナルは、リテイル銀行店などの物理的に安全な場所に位置する。

ＤＰＣがＢＩＡ／Ｒｅｇ登録リクエストに確実に応答するためには、３つのエンティティ：登録する従業員、機関およびＢＩＡ／Ｒｅｇが識別される必要がある。従業員は、個人をその機関に登録するためには承認されていなければならない。

機関およびＢＩＡは、ＢＩＡの所有者とＢＲＴによって設定された機関コードとをクロスチェックすることにより識別される。従業員は、登録アプリケーションを開始させる際に自分のバイオメトリックＰＩＣを入力することにより、システムに対して自分を識別させる。

機関は、個人をシステムに登録する前に、標準顧客識別プロシージャ（署名カード、従業員記録、個人情報など）を用いる。登録する個人は、随意にアカウン

トから金銭を転送および／または電子メッセージを会社の名前を使って送る権限を与えられるので、機関にとって個人の同一性をできる限り根気強く検証することが重要である。

登録する間に、個人は第一次および二次のバイオメトリックの両方を入力する。個人は、両方の人差し指を使用しなければならず、個人に人差し指がない場合には、隣りの親指が使用され得る。特定の指が使われることを要求することにより、以前の詐欺のチェックを行うことが可能となる。

個人は、第１の指および第２の指を選択することを奨励され、ＤＰＣ同一性チェックの間、第１の指が優先されるので、個人は、第１の指として、最もよく使う指を示すべきである。もちろん、ＤＰＣは、そうすることが重要であると判明すれば、操作に基づく第１および第２のバイオメトリックスの指定を変更することを選択することも可能である。

バイオメトリックコード化プロセスの一部として、ＢＩＡ／Ｒは、個人が「良い指紋」を入力したかどうかを決定する。研磨剤または酸を用いて働く個人など、仕事が、結果として偶発的な指紋の除去につながる個人もいることに注意されたい。残念なことに、これらの個人は、このシステムを使用することができない。彼らは、プロセスのこの段階で検知され、関与できないことを告げられる。

個人は、システムの中心データベースによって提供される一連のＰＩＣオプションから、４から１２桁からなるＰＩＣを選択する。しかし、ＰＩＣは、システムによって有効性を証明されなければならない。これは、２つのチェックを伴い、１つは、（ＰＩＣは、バイオメトリック比較アルゴリズムによってチェックされる個人の数を減らすために使用されるので）同じＰＩＣを用いる他の個人の数が多すぎないこと、そして、生物測定的にいって、登録されている個人が、同じＰＩＣグループの他の個人とあまりにも「近く」ないことである。どちらかが起こった場合、登録は拒否され、エラーメッセージがＢＲＴに戻され、個人は異なるＰＩＣをリクエストすることを指示される。このシステムは、個人がＰＩＣ下の

システムにおいて記録をすでに有することを示す「同一性一致」エラー状態を、

任意に返答し得る。

０のＰＩＣにより、システムがＰＩＣを個人に割り当てることが可能となる。

個人は、ワードまたはフレーズからなる秘匿性秘密コードを作成する。個人がそれを作成することを望まない場合は、秘密コードが、ターミナルによってランダムに作成される。

個人は、その金融資産コードリストをアレンジすることもできる。このリストには、どのアカウントインデックスコードがどのアカウント（即ち、１．借方、２．貸方、３．緊急借方、等）を指しているのかが記されている。これは、登録機関が銀行であり、且つ、アカウントがその特定の銀行機関によって所有されている場合にのみ行われ得る。

登録後であっても、以前の詐欺のチェックが完了するまでは、システムを使用して実際に処理を行うことはできない。一般に、これにかかるのは数分であるが、ハイロードの時間帯には最高数時間かかる。システムが以前の詐欺の事例が全くないことを認めるまでは、その個人のアカウントはアクティベートされない。

個人が、それまでに１回でもシステムを詐取したことがあると認められた場合、ＤＰＣは、その犯罪者について、全データベース強制バイオメトリックデータベースサーチ(database-wide involuntary biometric database search)を開始する。これらの中のいくつかは毎晩行われ、軽いアクティビティ条件の間に(during conditions of light activity)時間のかかる処理を行うことによって、システムから特に指名手配されている個人がデータベースから吹き飛ばされる。

ターミナル：顧客サービス

顧客サービスターミナル（ＣＳＴ）の目的は、内部のＤＰＣサポート職員に、システムデータベースの様々な局面へのアクセスを提供することである。サポート係は、システムに関するトラブルをかかえる個人、発行者、機関、およびマーチャントの問い合わせに答えなければならない。

ＣＳＴの構成：

・マイクロコンピュータ

・ＢＩＡ／Ｉｎｔ

・イーサネット／トークンリング／ＦＤＤＩネットワークインターフェース

・データベース検査および改変用アプリケーション

各ＣＳＴは、トークンリング、イーサネット、ファイバ（ＦＤＤＩ）等の高速ローカルエリアネットワーク接続を介してシステムに接続される。各ＣＳＴは、データベースのそれぞれに対して照会を行って、その照会結果を表示することができる。但し、ＣＳＴは個々のターミナルユーザの特権に基づいたフィールドおよび記録だけを表示する。例えば、標準的な(standard)顧客サービス従業員は、そのＢＩＡを現在どのマーチャントあるいは個人が所有しているのかを見ることはできるが、所与のＢＩＡのＶＤＢ記録の暗号化コードを見ることはできない。

ＣＳＴによってデータベースへのアクセスが許可されるには、その個人およびそのＢＩＡがシステムによって識別されなければならない。さらに、データベースがアクセスを適切に制限するためには、その個人の特権レベルも決定されなければならない。

ＣＳＴを使用する個人は、そのバイオメトリックＰＩＣを入力して識別子を提供することによってセッションを開始する。ＢＩＡは、認識リクエストメッセージを作成して、それを、検証のためにＤＰＣに送信する。システムがその個人を検証すると、ＣＳＴアプリケーションは、予め指定されたその個人のＤＰＣ特権レベルによって制限されるものの、通常処理を行うことができるようになる。

故意に、あるいは知らない間にウィルスが導入される等、いかなる方法によってもデータベースアプリケーションが改変されないことが重要である。この目的のために、個々のＣＳＴには、フロッピードライブや他の取り外し可能な媒体が全くない。さらに、実行可能なデータベースアプリケーションへの読出しアクセスは、知る必要性のある者だけにきびしく限定される。

不正な改変や漏洩(disclosure)からＣＳＴおよびデータベース間の通信を保護するために、ＣＳＴは、ＣＳＴおよびデータベース間のトラフィックを全て暗号化する。これを行うために、ＣＳＴはセッション鍵を生成する。この鍵は、システムとのログインセッションの間にサーバに送信される。このセッション鍵を用いて、期間中に生じるＤＰＣとの全通信の暗号化および復号化を行う。

通信が安全であり、データベースアプリケーションの改変が全くないと仮定した上で、ＤＰＣは、ＣＳＴを使用している個人にはアクセス不可能なＤＰＣデータフィールドがＣＳＴデータベースアプリケーションに送信されることがないようにする。同様に、どの時点においても、いかなるＣＳＴ職員にも、個人のバイオメトリック情報を改変するためのアクセスあるいは許可は与えられない。

ＤＰＣとサポートセンタとは同じ場所にあってもよいし、あるいは、ＣＳＴ周辺のセキュリティはかなり厳重であるので、サポートセンタを分けて独立させてもよい。

ターミナル：発行者ターミナル

発行者ターミナルの目的は、発行銀行(issuing banks)の従業員が、ＤＰＣに対するバッチ資産アカウント改変処理の入力を安全且つ識別可能に行うことができるようにすることである。

ＩＴの構成：

・マイクロコンピュータ

・モデム、Ｘ．２５ネットワーク、あるいはシステムへのインターネット接続

・ＢＩＡ／Ｉｓｓ

・銀行の内部ネットワークへのネットワーク接続

発行者ターミナルは発行者ＢＩＡを用いて、金融資産情報に関する大量の追加および削除を承認する。

この処理においては、銀行が識別されなければならず、適正に承認された銀行の従業員が識別されなければならず、また、資産アカウントの追加または削除を行っている個人が全て識別されなければならない。

銀行は、銀行のアカウント(口座)を資産アカウントリストに追加しようとしている個人を識別する役割を有する。バイオメトリック登録の場合と同様に、これは、署名カードおよび個人情報を用いて銀行によって行われる。ＩＴによって入力された発行者コードとＢＩＡ／ＩｓｓのＶＡＤ記録内に登録されている発行者コードとをクロスチェックすることによって、ＤＰＣは銀行を識別する。バイオメトリックＰＩＣを用いて、そのバッチを実際に入力している銀行の従業員を識

別する。

金融資産アカウントを追加する際、個人は、追加するアカウント(口座)と一緒に、その個人のバイオメトリック識別番号を銀行に与える（この識別番号は、初めのバイオメトリック登録ステップの際に個人に与えられる）。個人が適切に識別された後、この識別コードおよびアカウントリストをＩＴにフォワードして、それ以降のバッチのシステムへの入力を行う。

銀行が適切であると認める場合はいつでも、銀行の承認された個人は、ＩＴに命令を与えて、ＤＰＣへのバッチ化されたアカウント追加／削除をアップロードさせる。これを行うために、承認された個人はバイオメトリックＰＩＣを入力し、ＩＴはセッション鍵の追加および銀行の発行者コードの追加を行い、これにより、ＢＩＡ／Ｉｓｓは、発行者バッチリクエストメッセージを作成し、その後、ＩＴはこれをＤＰＣにフォワードする。ＩＴは、メッセージコードを用いてそのバッチを暗号化した後、その送信も行う。

システムは、発行者バッチリクエストを受信すると、そのＢＩＡがＢＩＡ／Ｉｓｓであること、そのＢＩＡ／Ｉｓｓが発行者コードによって要求されている銀行に登録されていること、ならびに、そのバイオメトリックＰＩＣにおいて識別される個人がその銀行についてＤＰＣにバッチリクエストを入力することを許可されていることを確認する。そうである場合、ＤＰＣは、必要に応じてエラーの記録をとりながら、全てのリクエストを処理する。これが終了すると、ＤＰＣは、処理中に生じた全てのエラーを有する暗号化されたバッチと一緒に、個人の秘密コードを返す。

このシステムのセキュリティにとって、このトランザクションのセキュリティは決定的である。詐欺行為をしようとする悪意があれば、他人のアカウントを自分のバイオメトリック識別コードに追加する方法を見つけるだけで、思いのままに詐欺行為を行うことができるようになる。最終的には、その犯罪者はとらえられて、データベースから一掃されるのだが、それは、その犯罪者が他人のアカウントを空にしてからのことである。

銀行とＢＩＡ／Ｉｓｓとをクロスチェックするということは、ＩＴおよびＢＩ

Ａが共に偽の追加／削除メッセージをＤＰＣに入力するようにしなければならないことを意味する。従って、銀行は、ＩＴが物理的に安全であり、且つそのアクセスが承認された個人だけに許可されていることを確実にしなければならない。

ターミナル：自動預金支払機(Automated Teller Machinery)

バイオメトリックＡＴＭの目的は、インターバンクカード(interbank card)を用いる必要なく、現金へのアクセスおよび他のＡＴＭ機能を個人に提供することである。これは、バイオメトリックＰＩＣおよびアカウントインデックスコードを入力して、銀行口座番号を取り出すことによって行われる。システムのユーザにとって、これは、インターバンクカード（当該分野では公知）＋口座を識別して個人を承認するための方法としてのＰＩＣメカニズムにとって代わるものである。全てのＡＴＭが依然としてインターバンクカードを受けつけるものと仮定する。

ＡＴＭの構成：

・標準的なＡＴＭ

・一体型ＢＩＡ／ＡＴＭ（スキャナのみ）

・ＤＰＣへの接続

バイオメトリックＡＴＭは、一体型ＢＩＡ／ＡＴＭを用いて、個人を識別するとともにその個人がバイオメトリックＰＩＣおよびアカウントインデックスを用いて金融資産にアクセスできるようにする。ＢＩＡ／ＡＴＭはＡＴＭ内に設置され、ＰＩＣおよびアカウントインデックスコードの入力用には、既存のＡＴＭのＰＩＣパッドを利用する。ＡＴＭは、Ｘ．２５あるいはモデムを用いてシステムに接続される。

ＢＩＡ／ＡＴＭは、現存のＡＴＭネットワークとの一体化ができるだけ簡単になるように構成される。ＤＰＣがＢＩＡ／ＡＴＭアカウントリクエストに適切に応答するためには、次のエンティティが識別される必要がある：個人、銀行およびＢＩＡ／ＡＴＭ。

ＡＴＭの格納銀行コードとＢＩＡ／ＡＴＭの銀行コードとをクロスチェックすることによって、銀行が識別される。ＢＩＡ／ＡＴＭは、ＶＡＤ内におけるＢＩ

Ａ／ＡＴＭの特定が成功することによって識別され、個人は、標準的なバイオメトリックＰＩＣによって識別される。

ＡＴＭにアクセスするために、個人は、アカウントインデックスコードと共に、バイオメトリックＰＩＣをＢＩＡに入力する。ＢＩＡは、アカウントアクセスリクエストメッセージを作成し、このアカウントアクセスリクエストメッセージはその後ＡＴＭによってＤＰＣに送信される。ＤＰＣは、緊急アカウントインデックスコードとともに、バイオメトリックＰＩＣの有効性を証明し、その後、得られた資産アカウント番号を秘密コードと一緒にＡＴＭに送り返す。

ＡＴＭは、ＢＩＡにレスポンスを復号化するように要求し、その後、ＡＴＭのディスプレイスクリーン上に秘密コードを表示する。また、ＡＴＭはレスポンスを検査して、その個人が標準的なアカウントアクセスを行っているのか、それとも、「脅迫(duress)」アカウントアクセスを行っているのかを確認する。脅迫アカウントアクセスであることが分かると、ＡＴＭは、その個人が利用可能である金額に関する偽あるいは誤解させるような情報を提供してもよい。この動作の詳細はＡＴＭによって異なる。但し、いかなるＡＴＭも、脅迫トランザクション(duress transaction)が進行中であることをその個人に示すことはない。

ＡＴＭおよびＤＰＣ間のメッセージの安全性は、暗号化およびＢＩＡからのＭＡＣ計算によって保たれる。ＭＡＣは、ＡＴＭが検知されずにメッセージのコンテンツを変更することはできないことを意味し、暗号化はそのメッセージの暗号化された部分の漏洩を防ぐ。

ＢＩＡ／ＡＴＭには、ＬＣＤやＰＩＣパッドが付いていないので、ＡＴＭには、あらゆるテキストプロンプトを提供して、その個人からの入力を全て集めることが要求される。これは、ＢＩＡによってこの処理を行う場合に比べて比較的安全

でないが、一般にＡＴＭは物理的に頑丈であるので、おそらく問題にはならないとされるであろう。

偽のスクリーンは、不正確になるように意図的に予め決められたデータの表示であるので、脅迫者が、ある個人の金融資産についての正確なデータを不法に入

手することはない。

ターミナル：電話ＰＯＳターミナル

電話ＰＯＳターミナル（ＰＰＴ）の目的は、特別装備の電話を用いてマーチャントからの購入を行う個人からの貸方あるいは借方金融トランザクションを承認することである。

ＰＰＴの構成：

・ＢＩＡ／ｃａｔｖ

・高速接続デジタルモデム［VoiceView特許（当該分野では公知）を参照］

・電話（キーパッド、受話器、マイク）

・マイクロコンピュータ

・ＤＳＰ（デジタル信号プロセッサ）

・標準的な電話線

ＰＰＴは、コードレス電話、セルラー電話、あるいは標準的な電話に接続され一体化されたＢＩＡ／ｃａｔｖを用いて、バイオメトリック識別子を受け付ける。

ＤＰＣがトランザクションを承認するためには、個人およびマーチャントの両者を識別しなければならない。個人を識別するために、バイオメトリックＰＩＣ識別が用いられる。

電話注文マーチャントを識別するために、マーチャントと、個人がかけるマーチャントの電話番号の全てをＤＰＣに登録する。従って、個人は、承認を入力する際に、その個人がかけた電話番号も入力する。その後、この電話番号を、マーチャントの電話番号リストとクロスチェックする。

個人は、紙のカタログ、新聞、雑誌、あるいは他の基本的な印刷媒体メカニズムを用いて商品を販売しているマーチャントに電話をかける。ＰＰＴは、電話音声ラインを共有する専用モデムを用いて、マーチャントとデジタル情報を交換する。

個人が電話をかける度に、個人が購入を決定した場合のために、ＰＰＴは、ユーザによって押された電話番号の記録をとる。ＤＳＰを用いて、発信音、呼出し

音(ring)、接続(connection)等を検知し、これにより、内線、あるいは電話メッセージシステムの案内等と区別して、入力された実際の電話番号が何であったのかを知る。

マーチャントに電話がかかると、そのマーチャントの販売員は、商品、価格、およびマーチャントコードを含む関連する情報を全てＰＰＴにデジタル方式でダウンロードする。使用中、モデムはスピーカを切る(disconnect)ことに留意されたい。

商品情報がダウンロードされると、その後、ＰＰＴは個人にプロンプトを出してバイオメトリックＰＩＣ、アカウントインデックスコードを促し、その後、個人に購入金額の有効性を証明するように要求する。その後、電話番号およびマーチャントコードを追加して、メッセージを暗号化する。高速接続モデムを再び用いて、マーチャントに承認情報を送信する。

マーチャントは、承認情報を受信すると、価格および商品情報が正しいことを検証し、その後、インターネットあるいは他の汎用ネットワークを用いた安全な通信チャネルを使って、トランザクションをＤＰＣにフォワードする。公開鍵暗号化および秘密鍵交換を用いて、ＤＰＣへの接続の安全性が保たれる。

電話承認の受信および復号化の際に、ＤＰＣはマーチャントコードに対してその電話番号をチェックし、そのバイオメトリックＰＩＣの有効性を証明し、その後、トランザクションを承認のために貸方／借方ネットワークに送信する。承認が成功すれば、ＤＰＣは購入者のアドレスをレスポンスメッセージに添付し、そのレスポンスをマーチャントに送信する。

マーチャントは、ＤＰＣからレスポンスを受信し、その宛先をコピーし、そして、高速接続モデムを用いた短時間のセッションによってメッセージを再び個人にフォワードする。ＩＰＴへの送信が完了すると、チャイムが鳴り、モデムを切

断し、個人の秘密コード（ＢＩＡによって復号化）をＬＣＤスクリーン上に表示する。マーチャントの販売代理人は、個人の宛先が有効であることを確認し、有効であれば電話を切ってトランザクションを完了する。

ターミナル：ケーブルＴＶＰＯＳ

ＣＡＴＶ販売時点情報管理ターミナル（ＣＰＴ）の目的は、テレビ受信機（または「ＴＶ」）の前にいる個人から、テレビ放送で商品を紹介しているマーチャントへの貸方または借方財政的トランザクションを承認することである。

ＣＰＴの構成：

・ＢＩＡ／catv

・集積型ＢＩＡ／catvを有するテレビのリモコン

・ケーブルＴＶデジタル信号デコーダ

・ケーブルＴＶリモコン読み取り装置

・オンスクリーン表示メカニズム

・ケーブルＴＶ広帯域双方向通信チャンネルへのアクセス

ＣＰＴは、テレビのリモコンデバイスに組み込まれたＢＩＡ／catvを用いて、バイオメトリック識別を受け取る。リモコンは、それ自体が広帯域ケーブルテレビネットワークと通信するテレビのトップボックスと通信する。ターミナルは、ＢＩＡと通信するテレビ遠隔ロジックおよびケーブル広帯域ネットワークで通信するテレビのトップボックスを含む。

このトランザクションにおいて、トランザクションを実行するためには、マーチャントおよび個人は共に識別されなければならない。個人は、バイオメトリックＰＩＣによって識別される。マーチャントは、製品がテレビ放送で見せられる時にＣＡＴＶ放送局によって作成されるマーチャントクリデンシャルによって識別される。各製品の放送は、マーチャントコード、時刻、持続期間、および公開鍵暗号化とＣＡＴＶネットワーク放送局の秘密鍵とを用いて署名される価格で構成されているマーチャント製品クリデンシャルを有する。このマーチャント製品クリデンシャルは、ネットワーク放送局によってのみ作成され得る。

テレビ公告、インフォマーシャルまたはホームショッピングチャンネルは、製品を表示するので、ケーブルテレビネットワークも、簡単な説明、価格、およびマーチャント製品クリデンシャルを説明する同時デジタル情報を放送する。このデジタル情報はＣＰＴによって処理されて一時的に格納され、購入の決断がなされれば、個人によって直ちにアクセスできる。

現在表示されている物を購入するためには、個人は、ＣＰＴに命令を与えて、現在視聴している製品に関する文字情報をスクリーン上に表示させる専用テレビリモコンのオンスクリーン表示機能を選択する。

個人は、まず、オンスクリーンディスプレイを介して購入するアイテムの希望数の入力をプロンプトにより促される。次に、その個人のバイオメトリックＰＩＣ、およびその個人のアカウントインデックスコードの入力をプロンプトにより促される。その個人が最終購入額が適切であると検証するとすぐに、バイオメトリックＰＩＣとともに、製品、価格、マーチャントコード、マーチャント製品クリデンシャル、およびチャネル番号を使用して、遠隔トランザクション承認リクエストメッセージが作成される。このリクエストは、ケーブルテレビジョン広帯域双方向通信チャネルを用いて、承認のためにマーチャントに送信される。

このような手法で製品を購買することを望むマーチャントは、各自、広帯域ケーブルテレビジョンネットワークを使用して注文情報を受信することが可能である必要がある。

承認リクエストの受信に伴って、マーチャントはそれを、安全なインターネット接続またはX.25接続を使用してＤＰＣに入力する。

ＤＰＣがトランザクションを承認すると、承認コードに加えて個人の宛先、および暗号化された秘密コードを含む承認レスポンスを作成する。マーチャントは、承認を受信するとすぐに、承認、および郵送住所をコピーし、次に承認を転送してＣＰＴに戻し、次にＣＰＴは、個人に秘密コードを表示し、トランザクションを終了する。

このアーキテクチャは、犯罪者がケーブルＴＶ広帯域から受信したメッセージを再生することを許可しないが、彼らがそれらを部分的に読むことは可能である。これが望ましくない場合には、(業界で知られている)ＣＡＴＶセットトップボックスとＣＡＴＶローカルオフィスとの間で、オプションであるＣＡＴＶセンター

の公開鍵、または他の「リンクレベル」暗号化を使用して、メッセージを暗号化し得る。

マーチャントとＤＰＣとの接続を安全にするために、この接続は、公開鍵暗号化鍵交換システムを使用して予め交換された、毎日変更されるセッション鍵を使用する。

システム記述：データプロセッシングセンタ

データプロセッシングセンタ（ＤＰＣ）は、その責任下における主な仕事として、金融取引き承認（financlal transaction authorizations）と個人の登録とを扱う。さらに、ＤＰＣは、安全なファクス（secure faxes）、電子ドキュメントおよび電子署名のための、記憶と取出しとを提供する。

それぞれのＤＰＣサイトは、ＤＰＣ概略図（番号＊＊）に示されるように、ＬＡＮ（当該分野において公知）によって、ともに接続された多くのコンピュータおよびデータベースからなっている。複数の同一のＤＰＣサイトは、どの一つのＤＰＣサイトで、災害または深刻なハードウエアの故障に直面しても、信頼あるサービスを確実にする。さらに、それぞれのＤＰＣサイトは、電源バックアップおよびＤＰＣの重要なハードウエアおよびデータベースシステムの全てにおいて、複数の重複を有する。

ＤＰＣコンポーネントは、３つのカテゴリに分かれる。ハードウエア、ソフトウエアおよびデータベースである。下記は、カテゴリによる、それぞれのコンポーネントの簡潔な記述である。より詳細な記述は、次のセクションに現れる。

ＦＷ：

ファイアウオールマシン（Ｆirewall Machine）：ＤＰＣサイトのエントリ点。

ＧＭ：

ゲートウェイマシン（Ｇateway Machine）：システムコーディネータおよびメッセージプロセッサ。

ＤＰＣＬＡＮ

ＤＰＣローカルエリアネットワーク（ＤＣＰ Local Area Network）：ＤＰＣサイト

を接続する。

データベース

ＩＢＤ

個人のバイオメトリックデータベース（Ｉndividual Ｂirometric Database）：個人のバイオメトリックおよびＰＩＣコードから個人を識別する。

ＰＦＤ

以前の詐欺のデータベース（Ｐrior Ｆraud Ｄatabase）：システムに対して詐欺行為を行った個人をリストし、バイオメトリックがそれらの個人のいずれかに一致すれば、チェックすることができる。

ＶＡＤ

有効な装置のデータベース（Ｖalid Ａpparatus Ｄatabase）：ＢＩＡメッセージの有効性を検査し復号化するのに要求される情報を記憶する。

ＡＯＤ

装置のオーナーのデータベース（Ａpparatus Ｏwner Ｄatabase）：ＢＩＡデバイスのオーナーに関する情報を記憶する。

ＩＤ

発行者データベース（Ｉssuer Ｄatabase）：システムに参加する発行銀行を識別する。

ＡＩＤ

承認された個人データベース（Ａuthorized Ｉndividual Ｄatabase）：パーソナルまたは発行者ＢＩＡデバイスを用いることが許された個人のリストを記憶する。

ＲＭＤ

リモートマーチャントデータベース（Ｒemote Ｍerchant Ｄatabase）：電話およびケーブルテレビジョンマーチャントとともに取引を処理するために必要な情報を記憶する。

ＥＤＤ

電子ドキュメントデータベース（Ｅlectronic Ｄocument Ｄatabase）：承認された個人による取出しのために、ファクスおよび電子メール等の、電子ドキュメン

トを記憶する。

ＥＳＤ

電子署名データベース（Ｅlectronic Ｓignature Ｄatabase）：第３者による有効性証明のために、電子ドキュメント署名を記憶する。

ソフトウエア

ＭＰＭ

メッセージプロセッシングモジュール（Message Processing Module）：他のソフトウエアモジュールとメッセージのタスクを実行するために要求されるデータベースとに整合することで、それぞれのメッセージのプロセッシングを取り扱う。

ＳＮＭ

シーケンス番号モジュール（Ｓequence Number Module）：ＤＵＫＰＴシーケンス番号プロセッシングを取り扱う。

ＭＡＣＭ

メッセージ承認コードモジュール（Message Authentication Code Module）：ＭＡＣの有効性の証明および生成を取り扱う。

ＭＤＭ

メッセージ復号化モジュール（Message Decrypt Module）：ＢＩＡ要求およびレスポンスの暗号化および復号化を取り扱う。

ＰＧＬ

ＰＩＣグループリスト（ＰＩＣ Ｇroup Ｌist）：ＰＩＣと、ＰＩＣグループのリストに依存するデータベースエレメントの構成とによって、ＰＩＣグループのルックアップを取り扱う。

ＩＭＬ

ＩＢＤマシンリスト（ＩＢＤ Machine Ｌist）：所定のＰＩＣグループのためにＩＢＤレコードを保持することを専門とした、メインおよびバックアップデータベースマシンのルックアップを取り扱う。

術語

データベースのスキーマ（schema）を定義する際に、次の術語がフィールドタイプを記述するために用いられる。

int〈X〉	〈X〉バイトの記憶を用いる整数タイプ
char〈X〉	〈X〉バイトの文字列
テキスト	可変長文字列
〈タイプ〉[X]	特定のタイプの長さ〈X〉の配列
時間	時間および日付を記憶するために用いられるタイプ
バイオメトリック	バイオメトリックを記憶するために用いられるバイナリデータタイプ
ファクス	ファクス画像を記憶するために用いられるバイナリデータタイプ

データベースの記憶要件を記述する際に、語「expected」は、完全にロードされたシステムの予想される状況を意味する。

プロトコルの説明

ターミナルは、DPCサイトにリクエストパケットを送信することによってそのタスクを成し遂げる。DPCサイトは、そのリクエストの成功または失敗に関するステータスを含む応答パケットを送り返す。

通信は、X.25接続、TCP/IP接続、またはモデムバンクへの電話呼出などの論理的または物理的な接続によるメッセージ配送メカニズムを介して行われる。各セッションでは、DPCがその応答をターミナルに送り返すまでターミナルへの接続が保持される。

リクエストパケットは、BIAメッセージ部およびターミナルメッセージ部を含む。

BIAメッセージ部

プロトコルバージョンNo.

メッセージタイプ

４－バイトBIA識別

４－バイトシーケンスNo.

〈メッセージ特定データ〉

メッセージ認証コード（MAC）

ターミナルメッセージ部

〈ターミナル特定データ〉

BIAメッセージ部は、BIAデバイスによって作成される。BIAメッセージ部は、１つまたは２つのバイオメトリック、PIC、承認量、およびターミナルによって設定される一般的なレジスタのコンテンツを含む。

注：BIAメッセージ部のMACは、BIA部にのみ適用され、ターミナル部には適用されない。

ターミナルは、リクエストメッセージに関する他のデータをターミナルメッセージ部に配置し得る。BIAは、メッセージ鍵を提供し、ターミナルがターミナル部データを確保できるようにする。BIAは、必要に応じて、メッセージ鍵をパケットの暗号化バイオメトリックーPICブロックに自動的に含む。しかし、ターミナルは、メッセージ鍵暗号化自体を実施する。

レスポンスパケットは、標準ヘッダと、MACを有する部およびMACを有さない部の２つのオプショナルフリー形態のメッセージ部とを含む。

標準ヘッダ

プロトコルバージョンNo.

メッセージタイプ

〈メッセージ特定データ〉

MAC

MACを有さないオプショナルフリー形態のメッセージ部

〈他のメッセージ特定データ〉

MACを有するメッセージ部は、BIAに送信され、この部分の応答に不正変更が加えられず、個人の秘密コードが表示されていないことの有効性を証明し得る。MACを有さないメッセージ部は、BIAのターミナル接続の帯域が限定され得るため、

MAC有効性の証明のためにBIAに送信されないファックス画像などの大量のデータを送信するために用いられる。

処理パケット

多数のDPCサイトを有する本発明の実施態様において、ターミナルは、そのリクエストをDPCサイトの１つ（通常最も近いサイト）にのみ送信する必要がある。なぜなら、そのサイトは、必要に応じて、配布されたトランザクションを実行することによってその他のサイトの更新を自動的に取り扱うからである。

DPCのファイアウォールマシン（Firewall Machines）の１つがパケットを受信すると、そのマシンはそのパケットをGMマシンの１つにフォワードして実際の処理を行う。各GMは、リクエストを処理するために必要なDPC構成要素間の協調を取り扱い、応答を送信者に送り返すメッセージ処理モジュールを有する。

パケットの有効性の証明および復号化

DPCが受信するBIAによって作成されないパケットを除くすべてのパケットは、BIAハードウェア識別コード（パケットのBIA識別）、シーケンスNo.、およびメッセージ認証コード（MAC）を含む。GMは、MACモジュールにパケットMACの有効性を証明するように要求し、次に、シーケンスNo.モジュールを用いてシーケンスNo.をチェックする。この２つが確認されると、GMは、パケットをメッセージ復号化モジュールに送りパケットを復号化する。いずれか１つが確認されない場合には、GMは、警告をロッグし、パケットの処理を停止し、エラーメッセージをBIAデバイスに戻す。

現在、BIAによって作成されないメッセージタイプは、安全ファックスデータリクエストおよび電子文書データリクエストのみである。

応答パケット

DPCが受信する各パケットは、パケットの暗号化バイオメトリック－PICブロックに格納されるオプショナル応答鍵を含んでいてもよい。DPCは、応答鍵を含むリクエストに応答する前に、応答パケットを応答鍵で暗号化する。さらに、DPC

は、メッセージ認証コードを生成し、それをパケットに追加する。

レスポンスパケットを暗号化しない唯一の例外としてエラーメッセージが挙げられる。エラーは暗号化されず、機密情報を含まない。しかし、大抵のレスポンスパケットは、リクエストが成功したか否かを示すことができるステータスまた

は応答コードを含む。例えば、DPCがクレジット認証を拒否するとき、DPCはエラーパケットを戻さずに、「失敗（failed）」と設定された応答コードを有する通常のトランザクションレスポンスパケットを戻す。

DPCプロシージャ

DPCは、リクエストを処理する間に通常用いられる２つのプロシージャ、即ち、個人識別プロシージャおよび緊急応答プロシージャを有する。

個人識別プロシージャ

DPCが個人を識別することを要求するリクエストの場合、DPCは、以下のプロシージャを実行する： DPCは、 PICコードを用いて、IBDマシンリストをサーチしてこの与えられたPICコードに対する識別を取り扱う主要IBDマシンおよびバックアップIBDマシンを求める。次に、DPCは、主要マシンまたはバックアップマシンのいずれかのロードの少ない方に識別リクエストを送信する。IBDマシンは、個人に関するIBDレコードまたは「個人不明（individual no found）」エラーを用いて応答する。

IBDマシンは、与えられたPICに対するすべてのIBDレコードを取り出す。所有者バイオメトリックハードウェアデバイスを用いて、IBDマシンは、各レコードの第一のバイオメトリックと、個人のバイオメトリックとを比較し、これら２つのバイオメトリックの類似性を示す比較スコアに到達する。いずれのバイオメトリックも十分な類似性を有する比較スコアを有さない場合、第二のバイオメトリックを用いて比較が繰り返される。第２のバイオメトリックのいずれも十分な類似性を有する比較スコアを有さない場合、IBDマシンは、「個人不明」エラーを戻す。あるいは、IBDマシンは、秘密コード、アカウントNo.、タイトル、等のフィールドが得られる個人のIBDレコード全体を戻す。

緊急応答プロシージャ

アカウントインデックスを含むリクエストに関しては、DPCは、個人がその緊急アカウントインデックスを選択する場合を取り扱う。リクエストがDPCカスタマサポートスタッフに即座に通知するGM処理では、警告がロッグされ、レスポンスパケットが応答コードを有する場合、そのレスポンスパケットは「緊急」とし

て設定される。「緊急」応答コードに注意し、ATMターミナルセクションに記載されるような疑似スクリーンメカニズムなどのさらなる援助を提供するのは、リクエストを入力したBIAデバイスのオーナの責任である。DPCはまた、緊急アカウントインデックスがアクセスされる度に、個人のIBDレコードの緊急使用カウントを増加させる。

プロトコルリクエスト

以下のセクションでは、各プロトコルのリクエスト／応答およびそのプロトコルを実施するためにDPCが行うアクションについて記載する。

プロトコルパケットのリストは、

個人識別

トランザクション承認

登録

アカウントアクセス

発行者バッチ

安全ファックス入力

安全ファックスデータ

安全ファックス追跡

安全ファックス取り出し

安全ファックス拒否

安全ファックスアーカイブ

安全ファックス契約受理

安全ファックス契約拒否

安全ファックス機構変更

電子文書入力

電子文書データ

電子文書追跡

電子文書取り出し

電子文書拒否

電子文書アーカイブ

電子文書アーカイブ取り出し

電子署名

電子署名検証

ネットワーククリデンシャル

個人識別

個人識別リクエスト

BIA部：

４－バイトBIA識別

４－バイトシーケンスNo.

暗号化（DUKPT鍵）バイオメトリック－PICブロック

300－バイト承認バイオメトリック

４－12ディジットPIC

56-ビット応答鍵

MAC

ターミナル部：（使用されない）

個人識別応答

暗号化（応答鍵）：

秘密コードテキスト

個人名

バイオメトリック識別コード

MAC

個人識別リクエストは、バイオメトリック－ＰＩＣブロックを有し、DPCはこのブロックを個人識別プロシージャを用いて使用し、個人を識別する。個人が識別されると、DPCは、個人の名前、バイオメトリック識別、および秘密コードを用いて応答する。あるいは、DPCは、「個人不明」エラーを用いて応答する。

トランザクション承認

トランザクション承認リクエスト

BIA部：

４－バイトBIA識別

４－バイトシーケンスNo.

暗号化（DUKPT鍵）バイオメトリック－PICブロック：

300－バイト承認バイオメトリック

４－12ディジットPIC

56－ビット応答鍵

［オプショナル56－ビットメッセージ鍵］

アカウントインデックス

価格

マーチャント識別

［オプショナルフリーフォーマット製品情報］

［オプショナルマーチャントコード（電話＃、チャネル＃＋時間、店主名）］

［オプショナル送信アドレスリクエスト］

MAC

ターミナル部：（使用されない）

トランザクション承認応答

暗号化（応答鍵）：

秘密コードテキスト

承認応答

承認詳細（承認コード、トランザクション識別、等）

［オプショナル個人アドレス情報］

応答コード（失敗、ok、緊急）

MAC

２つの基本的なトランザクション承認サブタイプ、即ち、リテイル承認および遠隔承認がある。

リテイル承認に関しては、DPCは、リクエストのバイオメトリック－PICブロッ

クによって購入者個人を識別する。個人を識別することができない場合には、DPCは、「個人不明」エラーを用いて応答する。

次に、DPCは、外部承認リクエスト（BIAデバイスのオーナの資産アカウントに対する貸方の記入および個人資産アカウントに対する借方の記入）を、関係する資産アカウントのタイプ（ビザまたはアメリカンエキスプレスなど）に応じて、いくつかの現存する経済的承認サービスの１つに送信する。外部経済的承認サービスがトランザクションを認める場合、DPCは、外部承認コードおよび「ok」応答コードをBIAデバイスに戻す。あるいは、DPCは、承認が拒否された理由を戻し、応答コードを「失敗」に設定する。いずれにせよ、DPCは、応答中に個人の秘密コードを含む。

DPCが、リクエストのアカウントインデックスを用いて個人の資産アカウントを調べるとき、選択されたアカウントは、「緊急」のアカウントであり得る。このようなことが発生する場合、DPCは、緊急応答プロシージャに従う。しかし、それでも外部承認は発生する。

遠隔承認は、電話、メールオーダー、またはケーブルテレビマーチャントによって発生する。DPCは、以下を除いて、リテイル承認と同様に遠隔承認を取り扱う。

i）遠隔承認は、遠隔マーチャントコードを有し、DPCはこのコードを遠隔マーチャントデータベースと照合してチェックし、パケットのマーチャント識別がデータベースに格納されたものと一致するかどうかの有効性を検証する。さらに、貸方に記入された資産アカウントは、遠隔マーチャントのアカウントであって、

BIAデバイスのオーナのアカウントではない。

ii）さらに、遠隔承認を発生させるBIAデバイスは、個人のBIAデバイスである場合が多い。DPCは、BIAデバイスの使用を許可された個人の承認された個人データベースリストと照合して識別された個人のバイオメトリック識別をチェックする。個人がデバイスの使用を承認されていない場合には、DPCは、承認リクエストを拒否する。

iii）最後に、承認パケットは、「送信アドレス」インジケータを含み得る。こ

のインジケータは、DPCに個人のアドレスを応答パケットに含むように通知し、通常、メールオーダ購入に対してのみ使用される。

登録

登録リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ）バイオメトリック－ＰＩＣブロック：

1000-バイト　第１のバイオメトリック

1000-バイト　第２のバイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

56-ビット　メッセージ鍵

ＭＡＣ

ターミナル部：

暗号化された（メッセージ鍵）：

名前

住所

郵便番号

秘密コード

資産アカウントリスト（アカウントインデックスコード、アカウント番号）

緊急アカウント（アカウントインデックスコード、アカウント番号）

タイトルリスト（タイトルインデックスコード、タイトル名）

登録レスポンス

ステータスコード

暗号化された（レスポンス鍵）

秘密コードテキスト

ＰＩＣ

バイオメトリック識別コード

ＤＰＣ選出ＰＩＣリスト（元々選択されたＰＩＣが拒否された場合）

ステータスコード（ｏｋ、拒否）

ＭＡＣ

個人は、バイオメトリック登録ターミナル（ＢＲＴ）を通じてＤＰＣに登録を行う。ＢＲＴは、個人の名前、住所、金融資産アカウントのリスト、秘密コードおよび緊急アカウントといった付属的データとともに、第１のおよび第２のバイオメトリック、および個人識別コードを含む登録パケットをＤＰＣに送信する。任意に、個人は電子メールアドレス、ならびにタイトルおよびタイトルインデックスコードを有するタイトルリスト、さらに社会保障番号（すなわち「ＳＳＮ」）を含ませ得る。個人は、自分のＰＩＣコードを選んでもよいし、システムに選ばせてもよい。改変ステップにおいて、以前に入力されたいかなるデータも改変、または削除できる。

容易に実施できるように、どの所与の時点においても、登録サイトとして機能するのはある一つのＤＰＣサイトだけである。非登録ＤＰＣサイトが受け取った登録リクエストパケットは、現在の登録サイトにフォワードされる。登録ＤＰＣサイトは、登録チェック全体、ＩＢＤマシーンへのＩＢＤ記録の割り当て、および他の全てのＤＰＣサイトを更新するために必要な、ディストリビューティドトランザクション(distributed transaction)を行う。

登録ＤＰＣサイトは、他のＤＰＣサイトを更新するためにディストリビューティドトランザクションを実行する前に、登録リクエストに対して、ＰＩＣコードを指定していないものについて選出し、ＩＢＤ記録を（ＰＩＣグループリストにおいて指定される）メインおよびバックアップＩＢＤマシーンに格納し、ＰＩＣおよび登録パケットのバイオメトリック適合性をチェックする。

ＤＰＣは、個人識別コードおよびバイオメトリックサンプル複製チェックステップを実行し、登録ステップ中に集められたバイオメトリックスおよび個人識別コードを、同一の個人識別コードに現在関連づけられている、以前に登録された

全てのバイオメトリックスに対してチェックする。ＤＰＣは、次のような理由で登録を拒否し得る：ＰＩＣコードが一般的すぎる、あるいは、バイオメトリックスが、選ばれたＰＩＣ下に格納された他のバイオメトリックスと類似しすぎている。許容可能なＰＩＣを選ぶ際に個人を助けるべく、ＤＰＣは、それについては登録されることが確実に保証されるＰＩＣコードの短いリストを生成し、これを一定期間保存する。ＢＲＴは次に、個人にプロンプトを与えて、新しいＰＩＣの入力を促すか、この新しいＰＩＣは、上記適合ＰＩＣリストから選出されてもよい。

アカウント（口座）アクセス

アカウントアクセスリクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

［任意の56-ビット　メッセージ鍵］

アカウントインデックス

ＭＡＣ

ターミナル部：（不使用）

アカウントアクセスレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

［任意のＰＩＣ］

資産アカウント番号

返答コード（失敗、ｏｋ、緊急）

ＭＡＣ

アカウントアクセスリクエストにより、ＢＩＡを装備した自動預金支払機が、個人がＡＴＭに対して身分証明を行う、より安全で便利な方法を提供することが可能になる。

ＧＭは、パケットのバイオメトリックＰＩＣによって個人を識別し、指定されたアカウントインデックスを用いて、どの資産アカウント番号を取り出すのかを選ぶ。

リクエストのアカウントインデックスを用いて、ＧＭが個人の資産アカウントをルックアップするとき、選ばれたアカウントは、「緊急」アカウントであり得る。このことが起こった場合、ＧＭは緊急レスポンスプロシージャに従う。

発行者バッチ

発行者バッチリクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

56-ビット　メッセージ鍵

発行者コード

ＭＡＣ

ターミナル部：

暗号化された（メッセージ鍵）

ａｄｄ〈バイオメトリックＩｄ〉〈アカウントインデックス〉〈資産アカウント〉［〈緊急フラグ〉］

ｒｅｍｏｖｅ〈バイオメトリックＩｄ〉〈アカウントインデックス〉〈資産アカウント〉

発行者バッチレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

返答コード（失敗、ｏｋ、緊急）

ＭＡＣ

暗号化された（メッセージ鍵）失敗リスト：

失敗した〈コマンド〉〈コード〉

・・・

発行者バッチリクエストにより、発行銀行またはその他の機関が個人バイオメトリックデータベースのルーチン維持を行うことが可能になる。ＤＰＣはまた、ＤＰＣが非発行者ＢＩＡデバイスから発行者バッチリクエストを受け取った場合、セキュリティ違反警告(security violation warning)を記録し、またリクエストの処理を拒否する。

ＤＰＣは、個人識別プロシージャに従ってバッチリクエストを入力している個人を識別する。ＤＰＣは次に、個人が承認された個人データベースに登録され、送信発行者ターミナル内にあるＢＩＡデバイスを使用できる状態にあることをチェックする。

ＤＰＣはまた、リクエスト内の発行者コードを用いて発行者データベース内の装置所有者識別をルックアップし、それを有効装置データベース内に格納される装置所有者識別に対して比較して発行者コードが偽造されていないことを確認する。

ＤＰＣは次にメッセージ鍵により暗号化されたバッチリスト内のコマンドの追加および削除を実行する。バッチリストは、復帰改行分割コマンドリスト(newline separated list of commands)である。有効コマンドは以下のとおりである。

ａｄｄ（追加）〈バイオメトリックＩｄ〉〈アカウントインデックス〉〈資産アカウント〉［〈緊急フラグ〉］

追加コマンドは、指定されたアカウントインデックスのアカウントリストに資産アカウントを追加する。任意の緊急フラグは、特定のアカウントインデックスが個人の緊急アカウントとして取り扱われたかどうかを示す。現在アカウントリ

ストに格納されている資産アカウントが発行者のものではない場合、コマンドは失敗する。この特徴により、ある銀行が、個人の認知あるいは承認なしで他の銀行の顧客の資産アカウントを追加または除去することを防ぐ。

ｒｅｍｏｖｅ（除去）〈バイオメトリックＩｄ〉〈アカウントインデックス〉〈資産アカウント〉

除去コマンドは、アカウントリスト内の指定されたアカウントインデックスに格納された個人の資産アカウントを消去する。現在アカウントリストに格納されている資産アカウントが、発行者が除去しようとしているアカウントに一致しない場合、コマンドは失敗する。

正しく実行することに失敗したバッチ内のコマンド各々について、ＧＭがセキュリティ違反警告を記録し、失敗したレスポンスのリストにエントリを添付(appends)する。失敗したエントリは、コマンドのテキストおよびエラーコードを含む。

安全ファックス入力

安全ファックス入力リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックーＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

56-ビット　メッセージ鍵

セキュリティモード（保証無(unsecured)、送り手保証(sender-secured)、保証(secured)、保証秘匿(secured-confidential)）

送り手タイトルインデックスコード

送り手ファックス番号

送り手ファックス内線

受け手リスト

［任意のアーカイブファックスインジケータ］

［任意の契約／同意インジケータ］

ターミナル部：（不使用）

安全ファックス入力レスポンス

暗号化された（レスポンス鍵）

秘密コードテキスト

ファックストラッキング番号

ＭＡＣ

ＤＰＣが安全ファックス入力リクエストを受け取るとき、ＤＰＣは、個人識別プロシージャに従って、リクエストのバイオメトリック－ＰＩＣから個人を識別する。タイトルインデックスで記述された個人のタイトルとともに、この識別は受取人に提示され、そのことによってファックスの送り手は常時確実に識別される。

ＤＰＣがトラッキングの目的でトラッキング番号を生成し、そのトラッキング番号、送り手のバイオメトリック識別、セキュリティモード、およびメッセージ鍵を新しく作成されたＥＥＤ文書記録内に格納する。受け手リスト内の受け手各々に対して、ＤＰＣは、受け手記録も作成する。ＤＰＣは次に、送信中のファックスマシーンがこのメッセージ鍵で暗号化されたファックスデータを送信するのを待つ。

リクエストが「アーカイブファックス」または「契約／同意」インジケータを含んでいる場合、ＥＤＤは、文書および受け手記録のコピーをアーカイブデータベースに入れる。これらの記録への以降の更新は全て保存版(archived version)にされる。

ファックスデータは別のステップで送信され、これにより送り手がバイオメトリックおよびＰＩＣの入力を間違えた場合、ファックスマシーンに文書をフィードする時間を浪費する前にシステムが送り手に通知する。

安全ファックスデータ

安全ファックスデータリクエスト

ＢＩＡ部：（不使用）

ターミナル部：

ファックストラッキング番号

暗号化された（メッセージ鍵）：

ファクスイメージデータ

安全ファックスデータレスポンス

ステータス（未完、ｏｋ）

安全ファックスデータリクエストは、安全ファックスマシーンに、ファックスイメージをＤＰＣに送って前に指定した受け手への送信を行わせる。このリクエストは、安全にイメージを送信するために、バイオメトリック識別およびそれに代わるシークレットメッセージ鍵に依存するものを含んでいない。

ファックスイメージデータは、安全ファックス入力リクエストにより登録されるメッセージ鍵によって暗号化される。ＤＰＣがファックス全体を受け取ってしまえば、ＤＰＣは、各受け手のファックス番号へ安全ファックス着信通知(Secure Fax Arrival Notice)メッセージを送る。ＤＰＣは、ファックストラッキング番号を有する全ての受け手記録についてＥＤＤを照会することによって、受け手リストを取り出す。受け手記録はデスティネーションファックス番号および任意の拡張を有している。着信通知を送信後、ＤＰＣは、各受け手記録の送信ステータスフィールドを「通知済み」へと更新する。注：デスティネーションファックス番号がビジーの場合、ＤＰＣが送信ステータスフィールドに「ビジー」と記し、成功するまで通知を定期的（例えば１０分毎）に送信を再試行し、成功した時にはステータスフィールドを「通知済み」に更新する。

着信通知は以下のようなものである。

安全ファックス着信通知（ファックスメッセージ）

送り手の名前、会社名(company)、タイトル、およびファックス番号

ファックストラッキング番号

ファックスのダウンロード方法についての指示

ＤＰＣは、全ての受け手がファックスを取り出しまたは拒否した後にファックスを介して、送り手にステータス通知を送るだけである。送り手は、安全ファックストラッキングリクエスト（下記参照）を用いてＤＰＣを照会し、受け手全員の現在のステータスを得る。

安全ファックスステータス通知（ファックスメッセージ）

安全な送り手の名前、会社名、タイトル、およびファックス番号

ファックストラッキング番号

以下のものを示す受け手リスト：

名前、会社名、タイトル、およびファックス番号

送信データおよびステータス

契約／同意ステータス

ＤＰＣは、ＥＤＤ組織テーブル内の個人の会社名およびタイトル情報のそれぞれを検索する。システムに登録されておらず、従って安全ファックスを受け取ることができない個人、あるいは非受け手安全モードの場合、ＤＰＣは、安全ファックス着信通知を送らない。その代わりに、ＤＰＣは、ファックスを直接送る。ファックスラインがビジーの場合、ＤＰＣはファックスの送信に成功するまで１０分毎に再試行を行う。

ファックストラッキング

安全ファックストラッキングリクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

56-ビット　メッセージ鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックストラッキングレスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

トラッキングレスポンスファックスイメージのメッセージダイジェスト

ステータスコード（ｏｋ、失敗）

ＭＡＣ

受け手ステータスリストのファックスイメージ

ＤＰＣは、そのファックスについての全てのＥＤＤ受け手記録を引き出すことにより、および記録を表示するためのファックスメッセージを生成することにより、安全ファックストラッキングリクエストを処理する。トラッキングリクエストを行っている個人がファック文書の送り手ではない場合、ＤＰＣはステータスコードを失敗にセットし、レスポンスに空ファックスを入れる。

トラッキングレスポンスファックスは、受け手各々に対する送信ステータスを説明する情報を含んでいる。このファックスは、ラインビジー、ファックス着信通知送信済み、ファックス送信済み、ファックス拒否、契約受諾、などのステータス情報を含んでいる。

トラッキング通知は以下のとおりである。

安全ファックストラッキング通知（ファックスメッセージ）

送り手の名前、会社名、タイトル、およびファックス番号

ファックストラッキング番号

以下のものを示す受け手リスト：

名前、会社名、タイトル、およびファックス番号

送信データおよびステータス

契約ステータス

安全ファックス取り出し

安全ファックス取り出しリクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックス取り出しレスポンス

暗号化された（レスポンス鍵）：

秘密コード

56-ビットメッセージ鍵

ステータス（未完、ｏｋ、受け手無効）

ファックスイメージのメッセージダイジェスト

ＭＡＣ

暗号化された（メッセージ鍵）：

ファックスイメージ

ＤＰＣはバイオメトリック－ＰＩＣを用いて、個人識別プロシージャに従って取り出しリクエストを行っている個人を識別する。その個人および指定されたファックスに関してＥＤＤ受け手記録が存在しない場合、ＤＰＣは、「受け手無効」ステータスを返す。

ＤＰＣは暗号化されたファックスイメージを、正しいファックストラッキング番号、および要求者に返信されるバイオメトリック識別とともにＥＤＤドキュメント記録から取り出す。

ファックスイメージは、ファックスが契約／同意のものかどうかを、および送り手の名前、会社名、タイトル、ファックス番号、および拡張(extension)を表

示するカバーページを含んでいる。

最後の受け手がファックスの受取りあるいは拒否のどちらかを完了すると、ＤＰＣは、そのファックスの送り手にファックスを介してステータス通知を送り（上記の安全ファックスデータ参照）、次に設定可能時間内にＥＤＤから文書および受け手記録を削除するように予定を立てる。この時間は、ファックスをアーカイブするかどうかを決定するのに十分な時間を受け手に与えるためのものである。

安全ファックス拒否

安全ファックス拒否リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックス拒否レスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（ｏｋ、受け手無効）

ＭＡＣ

ＤＰＣはバイオメトリック－ＰＩＣを用いて、安全ファックス拒否リクエストを行っている個人を識別する。ＤＰＣは、リクエストのファックストラッキング番号および個人のバイオメトリック識別によって鍵がかけられたＥＤＤ受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステ

ータスとともに失敗する。

最後の受け手がファックスの受取りあるいは拒否のどちらかを完了すると、ＤＰＣは、そのファックスの送り手にファックスを介してステータス通知を送り（上記の安全ファックスデータ参照）、次に設定可能時間内にＥＤＤからファックスおよびトラッキング記録を削除するように予定を立てる。この時間は、ファックスをアーカイブするかどうかを決定するのに十分な時間を受け手に与えるためのものである。

安全ファックスアーカイブ

安全ファックスアーカイブリクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックスアーカイブレスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（ｏｋ、個人無効）

ＭＡＣ

ＤＰＣはバイオメトリック－ＰＩＣを用いて、安全ファックスアーカイブリクエストを行っている個人を識別する。ＤＰＣは、リクエストのファックストラッキング番号および個人のバイオメトリック識別によって鍵がかけられたＥＤＤ受け手記録を検索する。この記録が見つからず、個人が送り手でも受け手の一人で

もない場合、リクエストは「個人無効」ステータスとともに失敗する。そうでなければＤＰＣは、ＥＤＤアーカイブデータベースの中に文書および受け手記録をコピーする。これら記録への以降の変更は全て、保存版へコピーされる。

安全ファックス契約受諾

安全ファックス契約受諾リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックス契約受諾レスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（ｏｋ、受け手無効）

ＭＡＣ

ＤＰＣはバイオメトリック－ＰＩＣを用いて、契約受諾リクエストを行っている個人を識別する。ＤＰＣは、リクエストのファックストラッキング番号および

個人のバイオメトリック識別によって鍵がかけられたＥＤＤ受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステータスとともに失敗する。そうでなければＤＰＣは、受け手記録の契約ステータスフィールドを「受諾」に更新し、またファックスの送り手に対してステータス通知を生成する（上記ファックスデータ参照）。

安全ファックス契約拒否

安全ファックス契約拒否リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

ファックストラッキング番号

ＭＡＣ

ターミナル部：（不使用）

安全ファックス契約拒否レスポンス

暗号化された（レスポンス鍵）：

秘密コード

ステータスコード（ｏｋ、個人無効）

ＭＡＣ

ＤＰＣはバイオメトリック－ＰＩＣを用いて、契約拒否リクエストを行っている個人を識別する。ＤＰＣは、リクエストのファックストラッキング番号および個人のバイオメトリック識別によって鍵がかけられたＥＤＤ受け手記録を検索する。この記録が見つからない場合、リクエストは「受け手無効」ステータスとともに失敗する。そうでなければＤＰＣは、受け手記録の契約ステータスフィールドを「拒否」に更新し、またファックスの送り手に対してステータス通知を生成する（上記ファックスデータ参照）。

安全ファックス組織変更

安全ファックス組織変更（安全ファックスメッセージ）

送り手の名前、会社名、タイトル、およびファックス番号

組織変更のリスト

組織変更は、安全ファックスメッセージを介してＤＰＣに入力される。顧客サ

ポートエンジニアが、その特定の会社に個人を登録することをそのリクエストを入力している個人が許可されているかを確認しながら、ファックスメッセージにおいてリクエストされた変更を入力する。このファックスは安全ファックスなので、送り手の同一性は送り手のタイトル同様、確証済みである。

電子文書入力

電子文書入力リクエスト

ＢＩＡ部：

4-バイト　ＢＩＡ識別

4-バイト　シーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリック－ＰＩＣブロック：

300-バイト　承認バイオメトリック

4-12ディジット　ＰＩＣ

56-ビット　レスポンス鍵

56-ビット　メッセージ鍵

受け手リスト

ＭＡＣ

ターミナル部：（不使用）

電子文書入力レスポンス

暗号化された（レスポンス鍵）：

秘密コードテキスト

トラッキング番号

ステータスコード（ｏｋ、受け手無効）

ＭＡＣ

ＤＰＣは、電子文書入力リクエストを受け取ると、個人識別プロシージャに従って個人を識別する。

ＤＰＣは次にＥＤＤ文書記録を作成し、そのＥＤＤ文書記録に固有トラッキング番号を割り当てる。ＤＰＣは、記録の送り手識別コードを初期化して、識別した個人のバイオメトリック識別コードとし、またメッセージ鍵を初期化して、そ

のリクエストのメッセージ鍵とする。

次にＤＰＣは、受け手各々について識別バイオメトリックデータベースをサーチし、各々一人についてＥＤＤ受け手記録を作成する。各記録を、トラッキング番号、受け手のバイオメトリック識別コード、および送信ステータス「未完」で初期化する。受け手が一人として見つからない場合、ＤＰＣは、「受け手無効」ステータスを返答する。

電子文書データ

電子文書データリクエスト

ＢＩＡ部：（不使用）

ターミナル部：

トラッキング番号

コマンド（アボートあるいはデータ）

［任意のメッセージオフセット］

完了指標(indication)

暗号化された（メッセージ鍵）：

メッセージ本文

電子文書データレスポンス

ステータス（未完、ｏｋ）

電子文書データリクエストにより個人が文書テキスト（一部またはそれ以上の部分）をＥＤＤに送って、受け手への送信を行うことが可能になる。このリクエストはバイオメトリック識別を全く用いず、代わりに、文書テキストを安全に送信するためのシークレットメッセージ鍵を用いている。

リクエストテキストは、ＥＤＤ文書記録に格納されるメッセージ鍵によって暗号化されたものと仮定され、この記録に既に格納されている文書テキストに添付される。

ＥＤＤは、「文書完全性」インジケータを伴うパケットを受け取ったとき、送り手が文書の送信を完了したことを知る。次にＥＤＤは、インターネット電子メールを介してその文書の受け手全員に着信通知を送り、受け手に待期文書がある

ことを知らせる。

着信通知は以下のとおりである。

電子文書着信通知（インターネットＥ－メールメッセージ）

送り手の名前、会社名、タイトル、およびｅ－メールアドレス

トラッキング番号

電子文文書の受信に関する指示

ＥＤＤはまた、ＥＤＤ受け手記録のステータスを「通知済」に更新する。全ての受け手がその電子文書の取出しあるいは拒否のいずれかを完了すると、ＤＰＣ0は、インターネット電子メールを介して、文書編成者(document originator)にステータス通知を送る。

ステータス通知は以下の通りである。

電子文書ステータス通知（インターネットＥメールメッセージ）

送り手の名前、会社名、タイトル、およびｅメールアドレス

トラッキング番号

各人の名前、会社名、タイトル、ｅ－メールアドレスを示す受け手のリスト

送信データおよびステータス

ＤＰＣは、ＥＤＤ組織テーブル内の個人の会社名およびタイトル情報の各々を検索する。

電子文書取り出し

電子文書取り出しリクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

トラッキング番号

ＭＡＣ

ターミナル部：（不使用）

電子文書取り出しレスポンス

暗号化（レスポンス鍵）：

秘密コード

５６ビットメッセージ鍵

ステータス（未完、ＯＫ、受け手無効）

ＭＡＣ

暗号化（メッセージ鍵）：

文書テキスト

ＤＰＣは、個人識別手続きに従って、電子文書取り出しリクエストを行っている個人を識別するためにバイオメトリックＰＩＣを使用する。

続いてＤＰＣは、トラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたＥＤＤ受け手記録を発見する。

記録が発見できなければ、リクエストは「受け手無効」ステータスをもって失敗となる。それ以外の場合には、ＤＰＣは文書のメッセージ鍵及び（メッセージ鍵によって暗号化されたままの）文書を要求人に送る。

そしてＥＤＤは、ＥＤＤ受け手記録ステータスを「取り出し済み」に更新する。すべての受け手が文書の取り出しあるいは拒否を行ったら、ＤＰＣは文書編成者（上記電子文書データ参照）にインターネット電子メールでステータス通知を送り、そして文書記録及び受け手記録（上記安全ファックス取り出し参照）の削除の予定をたてる。

電子文書拒否

電子文書拒否リクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

メッセージトラッキング番号

ＭＡＣ

ターミナル部：（不使用）

電子文書拒否レスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（ＯＫ、受け手無効）

ＭＡＣ

ＤＰＣは、個人識別手続きに従って電子文書拒否リクエストを行っている個人を識別するためにバイオメトリックＰＩＣを使用する。

続いてＤＰＣは、トラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたＥＤＤ受け手記録を発見する。

記録が発見できなければ、リクエストは「受け手無効」ステータスをもって失敗する。

ＥＤＤは、ＥＤＤ受け手記録ステータスを「拒否」に更新する。そしてＤＰＣは電子文書取り出しにおいて述べたものと同じ通知及び削除手続きを続いて行う。

電子文書アーカイブ

電子文書アーカイブリクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

トラッキング番号

ＭＡＣ

ターミナル部：（不使用）

電子文書アーカイブレスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（ＯＫ、個人無効）

ＭＡＣ

ＤＰＣは、個人識別手続きに従って電子文書アーカイブリクエストを行っている個人を識別するためにバイオメトリックＰＩＣを使用する。

ＤＰＣは、リクエストのトラッキング番号及び個人のバイオメトリック識別子によって鍵をかけられたＥＤＤ受け手記録を発見する。

記録が発見できず、その個人が送り主あるいは受け手の一人でない場合、リクエストは「個人無効」ステータスをもって失敗する。それ以外の場合には、ＤＰＣは文書及び受け手記録をＥＤＤアーカイブデータベースにコピーする。それ以降のこれらの記録に対する変更は、全て保存版にコピーされる。

電子文書アーカイブ取り出し

電子文書アーカイブ取り出しリクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

任意のタイトルインデックスコード、送信ファックス番号、内線

トラッキング番号

ＭＡＣ

ターミナル部：（不使用）

電子文書アーカイブ取り出しレスポンス

暗号化（レスポンス鍵）：

秘密コード

ステータスコード（ＯＫ、個人無効）

ＭＡＣ

ＤＰＣは、安全ファックスターミナルあるいは認可された（Certified）Ｅメールターミナルいずれからも、電子文書アーカイブ取り出しリクエストを受けうる。ＤＰＣは、アーカイブ取り出しリクエストを出している個人を判定するために、個人識別手続きを使用する。個人は送り主あるいは受け手の一人でなければならず、それ以外の場合は、ＤＰＣはステータスコードを「個人無効」とすることによって、リクエストを拒否する。しかし、アーカイブ文書が法人名を用いて送られたファックスであるならば、ＤＰＣは、その法人の位階制度上、より高い役職名を有する更なる個人にもアーカイブ文書の取り出しを許可する。

ＥＤＤはアーカイブデータベースを保持するが、データベースは、文書の元のトラッキング番号によってインデックスされ、ＣＤ－ＲＯＭやアーカイブ文書の取り出しにかなりの時間を要しうるテープのようなオフライン記憶媒体に格納される。その結果、ＤＰＣはアーカイブ文書をすぐに返送するのではなく、それに代えてＤＰＣが検索を開始したことを要求人に報告する。後日、ＤＰＣが検索を終えた時、もとの文書のフォーマットに応じて、ファックスやＥメールといった標準的な文書着信通知メカニズムによって、保存された文書が取り出せる状態にあることを要求人に通知する。ＤＰＣはＥＤＤアーカイブリクエスト記録を生成して、要求人についての情報を格納し、それによって、検索が終了した際、ＤＰＣはその文書を誰に送信すべきかを改めて知ることができる。

電子署名

電子署名リクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

文書名

文書ＭＤ５計算

ＭＡＣ

ターミナル部：（不使用）

電子署名レスポンス

暗号化（レスポンス鍵）：

秘密コードテキスト

署名文字列

ＭＡＣ

電子署名リクエストを処理するため、ＤＰＣはまず、バイオメトリックＰＩＣを用いてバイオメトリック識別を行う。そして、ＤＰＣはＥＳＤ記録を生成し、それに固有の署名識別コードを割り当て、記録の署名フィールドをそのリクエスト内の電子署名に設定する。そしてＤＰＣは、後の検証において提出されうる署名文字列を返す。

” 〈Dr. Bunsen HoneyDew〉 〈Explosions in the Laboratory〉 5/17/95 13:00 PST 950517000102”

電子署名検証

電子署名検証リクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

署名文字列

ＭＡＣ

ターミナル部：（不使用）

電子署名検証レスポンス

暗号化（レスポンス鍵）：

秘密コードテキスト

署名文字列

ステータス（検証済み、失敗）

ＭＡＣ

ＤＰＣはバイオメトリック識別を行い、署名文字列から署名トラッキングコードを抽出し、示されたＥＳＤ記録を取り出して、それが署名文字列に一致することを検証する。ＤＰＣは秘密コード及び署名の比較の結果を返す。

ネットワーククリデンシャル

ネットワーククリデンシャルリクエスト

ＢＩＡ部：

４バイトＢＩＡ識別

４バイトシーケンス番号

暗号化された（ＤＵＫＰＴ鍵）バイオメトリックＰＩＣブロック：

３００バイト承認バイオメトリック

４－１２ディジットＰＩＣ

５６ビットレスポンス鍵

アカウントインデックス

銀行コード

銀行ホストネーム

ターミナルポート及び銀行ポート（ＴＣＰ／ＩＰ　アドレス）

ＭＡＣ

ネットワーククリデンシャルレスポンス

暗号化（レスポンス鍵）：

秘密コード

署名（ＤＰＣ秘密鍵）：

クリデンシャル（時間、アカウント、ターミナルポート、銀行ポート）

銀行公開鍵

ステータスコード（ｏｋ，失敗）

ＭＡＣ

ＤＰＣはリクエストのバイオメトリックＰＩＣを用いて個人を識別し、特定されたインデックスに格納された個人の資産のアカウントを取り出す。アカウントインデックスが緊急アカウントなら、ネットワーククリデンシャルレスポンスステータスコードは「失敗」と設定され、クリデンシャルは生成されない。

ＤＰＣは現在時間、取り出された資産アカウント、ターミナル及び銀行のＴＣＰ／ＩＰアドレスを用いてクリデンシャルを作成する。そしてＤＰＣは公開鍵暗号化を用いてその秘密鍵でクリデンシャルに署名する。レスポンスはまた、銀行のパブリック鍵を含むが、これはＤＰＣが遠隔マーチャントデータベースから取り出したものである。

顧客サポート及びシステム管理メッセージ

ＤＰＣは内部メッセージに分類されるさらなるメッセージタイプを扱う。ＤＰＣは一般に、非ＤＰＣシステムからのこれらのメッセージを受け付けない。そのメッセージはデータベースベンダー特有である。しかし、内部ネットワークは更なるセキュリティのためＤＥＳ暗号化パケットを用いている。

顧客サポート及びシステム管理タスクは、データベースベンダーの照会言語及びアプリケーション開発ツールを用いて実行される。

顧客サービスタスク

・ＩＢＤ：記録の検索、起動、終了、削除、訂正

・ＡＩＤ：承認された個人の追加または、削除

・ＡＯＤ：記録の検索、追加、削除、訂正

・ＶＡＤ：記録の検索、起動、終了、削除、訂正

・ＲＭＤ：記録の検索、追加、削除、訂正

・ＰＦＤ：記録の追加、削除、訂正

システム管理タスク

・以前の詐欺チェックの実行

・有効なサイトリストの修正

・ログ情報（警告、エラー等）の要約

・ＰＩＣグループリストの修正

・パフォーマンス監視

・バックアップの実行

・クラッシュ回復手続き

・ＤＰＣサイトの時間同期化

・主要な登録サイトの変更

・シークレットＤＥＳ暗号鍵の変更

・古い文書トラッキング番号の削除

・ＢＩＡハードウェア識別コード、ＭＡＣ暗号化鍵及び、ＤＵＫＰＴベース鍵の三つ組みリスト生成。鍵読み込みデバイス用の暗号フロッピーへの格納。

ファイアウォールマシン

FWマシンは、ネットワークウイルスおよびコンピュータハッカーに対する第１線の防御を提供する。DPCサイトへの及びDPCサイトからのすべての通信リンクは、まず安全なFWマシンを通過する。インターネットーローカルネットルータであるFWマシンは、GMマシン用のメッセージを取り扱うにすぎない。BIA搭載ターミナルは、モデム、X.25、または他の通信媒体を介して単一のDPCサイトにパケットを送信する。DPCは、第三者に依存して、呼の量を取り扱うため、およびDPCバックボーンへデータを供給するために必要なモデムバンクを供給する。

DPCからDPCへの通信、主に配布されたトランザクションおよびシーケンスナン

バの更新のために、FWマシンは、２倍の長さのDES暗号化パケットを送出する。DPC LANコンポーネントが、暗号化および復号化を取り扱い、FWは、パケットを復号化する能力を有していない。

適切に構成されたネットワークスニファ(sniffer)は、FW用のバックアップとしての侵入者検出器として作用する。変則的なメッセージが検出された場合、侵入するメッセージはその全体が記録されて、オペレータに警告が発され、FWはスニファにより物理的にシャットダウンされる。FWは、内部ネットワークからインターネットのそれ以外の部分への送信を禁止する。

トランザクション承認要求は約400バイトを必要とし、登録パケットは約2KBを必要とする。１秒あたり1000個のトランザクション承認および１秒あたり１個の登録パケットを扱うために、FWマシンは１秒あたり約400KBを処理する能力がある（すべては当該分野で知られている）。

各DPCサイトは、第三者のモデムバンクおよび他のDPCサイトへの３つのT1接続を総合した帯域幅を必要とする。

ゲートウェイマシン

GMマシン(GM)は、FWマシンを介して、外界（BIA搭載ターミナルおよび他のDPC）をDPCの内部コンポーネントにリンクする。DPCは、複数、通常２つのGMを有する。

GMは、各BIA要求の処理を監督し、必要に応じて様々なDPCコンポーネントと通信し、要求の暗号化結果を送り手に送り返す。このタスクを行うソフトウェアは、メッセージプロセシングモジュールと呼ばれる。

GMは、それが受け取るすべての要求、および通信するコンポーネントからのいずれの警告をも履歴に残す。例えば、GMは、いずれの緊急アカウントアクセス、シーケンスナンバギャップ、および無効パケットをも履歴に残す。要求の処理は、GMが、他のすべてのDPCにおけるGMに、DPCデータベース内の変更を通知することを必要とする。これが起こると、GMは、遠隔データベースを更新するために、配布されたトランザクションを行う。

配布されたトランザクションは、２つのカテゴリ、すなわち、同期および非同

期に分類される。同期配布されたトランザクションは、パケットの処理を続ける前に、配布されたトランザクションの送信に関する最終決定がなされることを、GMが待つことを必要とする。非同期配布されたトランザクションは、GMが最終決定がなされることを待つことを必要とせず、配布されたトランザクションの送信に関する最終決定がなされたか否かにかかわらずGMが要求の処理を終了することを許可する。非同期配布されたトランザクションは、データベースの一貫性が絶対に必要な事項ではないデータを更新するために用いられるのみである。シーケンスナンバおよびバイオメトリックチェックサム記録は、非同期に行われ得、他方、インディビジュアルバイオメトリック記録などのデータベース記録の作成は行われ得ない。

同期配布されたトランザクションを実行する場合に、すべてのサイトがローカルにトランザクションの送信に関する最終決定をすることに成功し得る場合、要求を出すGMは、トランザクション全体が成功したと考えるのみである。そうでない場合、GMは、ローカルに変更を取り消して、トランザクションエラーによる要求を拒否する。

有効なDPCサイトのリストは、通常全てのサイトである。しかし、極端なサイト障害(failure)の場合、システム管理者は、有効なサイトのリストからそのサイトを手動で除去し得る。しかし、配布されたトランザクションのフェイラの最も可能性の高い原因は、いずれのDPC装置とも無関係な一時的なネットワークフェイラである。同期配布されたトランザクションを必要とする要求は、ネットワークの接続可能性が回復されるか、またはサイトが有効サイトのリストから除去されるまで、行うことができない。サイトが有効なサイトのリストに再び追加されることができる前に、システム管理者は、サイトのデータベースを現在アクティブなサイトのデータベースまで更新する。

各GMは、性能上の理由で、ローカルに以下のソフトウェアを実行する。

メッセージプロセシングモジュール

メッセージ認証コードモジュール

メッセージ復号化モジュール

インディビジュアルバイオメトリックデータベースマシンリスト

GMにより必要とされるメッセージの帯域幅は、FWマシンにより必要とされるものと同様である。FDDIネットワークインターフェースは、１秒あたり100Mビットを提供し、いずれの帯域幅の必要要件をも容易にカバーしている。

DPC LAN

DPCローカルエリアネットワーク(LAN)は、光ファイバトークンリングを用いて、DPCサイトのマシンを互いにリンクする。光ファイバトークンリングは、高域幅と良好な物理的安全性との両方を提供する。

DPC LAN上のマシンにより用いられるネットワークインターフェースは、暗号化鍵がない場合、パケットを盗み見ることまたは傍受することを無益にする暗号化ハードウェアを含む。暗号化鍵は、LAN上のすべてのマシン用のものと同一であり、暗号化ハードウェア内に格納される。

適切に構成されたネットワークスニファは、FW用のバックアップとしての侵入者検出器として作用する。変則的なメッセージが検出された場合、侵入するメッセージはその全体が記録されて、オペレータに警告が発され、FWはスニファにより物理的にシャットダウンされる。

メッセージプロセシングモジュール

メッセージプロセシングモジュール(MPM)は、要求パケット用の処理を扱う。MPMは、そのタスクを実行するために必要に応じてDPCの他のコンポーネントと通信する。マシン上にMPMが存在することにより、マシンはGMと呼ばれる。

MPMは、現在処理中の各要求の要求コンテキストを維持する。要求コンテキストは、要求を行っているターミナルに対するネットワーク接続を維持するために必要な情報、BIAデバイス情報、レスポンス鍵、およびレスポンスパケットを含む。

メッセージ認証コードモジュール

メッセージ認証コードモジュール(MACM)タスクは、送られてくるパケット上のメッセージ認証コードの有効性を証明すること、および送出されるパケットにメッセージ認証コードを付加することである。MACMは、BIAハードウェア識別コー

ドにより鍵をかけられた112ビットのMAC暗号化鍵のメモリ内ハッシュテーブルを維持する。

MACMは、パケットのMACの有効性を証明するようにという要求をGMから受け取ると、まずハッシュテーブル内のパケットのハードウェア識別コードを参照する。エントリがない場合、MACMはGMに「無効なハードウェア識別コード」エラーであると応答する。

そうでない場合、MACMは、112ビットの暗号化鍵を用いて、パケットのBIAメッセージ部のMACチェックを行う。MACチェックが失敗した場合、MACMはGMに、「無効なMAC」エラーであると応答する。そうでない場合、MACMは、「有効なMAC」メッセージであると応答する。

パケットがマーチャントコードを含む場合、MACMはさらに、ハッシュテーブル内のオーナ識別コードに照らしてマーチャントコードをチェックする。コードが合致しない場合、MACMは「無効なオーナ」エラーであると応答する。

MACMは、パケット用のMACを生成するようにという要求をGMから受け取ると、パケットのハードウェア識別コードを用いてMAC暗号化鍵を参照する。MACMは、MAC暗号化鍵で、MACを生成してパケットに付加する。MACMがハードウェア識別コードを見つけることができない場合、MACMは、代わりに、無効なハードウェア識別コードエラーであると応答する。

MAMCハッシュテーブルエントリは、以下を含む。

MACMエントリ：

hardwareID=int4

ownerID=int4

macEncryptionKey=int16

テーブルは、ハードウェア識別コードによりハッシュされる。

500万のBIA搭載デバイスがサービスを行っているとすると、ハッシュテーブルは、約120MBの記憶容量を必要とする。性能上の理由により、このハッシュテーブルは、メモリ内で完全にキャッシュされる。

MACMは、アクティブなBIAハードウェア識別コードおよびアクティブな装置オ

ーナを参照する記録を含むのみである。装置または装置オーナが一時使用不可能にされるか、またはシステムから削除される毎に、MACMはその識別コードを参照するエントリを除去する。装置がアクティベートされると、MACMはその装置用のエントリを追加する。

MAMCはまた、有効な装置データベースからMAC暗号化鍵をキャッシュする。システムはBIAの暗号化鍵が変更されることを許可しないため、MACMは暗号化鍵の更新を受け取ることに対して懸念する必要はない。

メッセージ復号化モジュール

メッセージ復号化モジュール(MDM)タスクは、DUKPTトランザクション鍵を再構築すること、およびそれによりパケットのバイオメトリック－PICブロックを復号化することである。メッセージ復号モジュール(MDM)は、トランザクション鍵を生成するために必要なDUKPTベース鍵のリストを維持する。

MDMは、DUKPTトランザクションカウンタとしてのパケットのシーケンスナンバ、DUKPT不正改変不可能な安全なモジュール(すなわち「TRSM」)識別子としてのBIAハードウェア識別コードの上位22ビット、およびDUKPT鍵セット識別子としてのBIAハードウェア識別コードの下位10ビットを用いて、DUPKTトランザクション鍵を再構築する。

DUKPT標準は、トランザクション鍵がどのように生成されるかを特定する。鍵セット識別子は、ベース鍵リストからベース鍵を参照するために用いられる。ベース鍵は、DES暗号化／復号化／暗号化のサイクルを介して、TRSM識別子を初期

鍵に変換するために用いられる。その後、トランザクションカウンタは、一連のDES暗号化／復号化／暗号化のサイクルとしての初期鍵を、トランザクション鍵を生成するために適用するために用いられる。

更なる安全性のために、２つのベース鍵リストが維持される。１つは低安全性BIAデバイス用であり、１つは高安全性デバイス用である。MDMは、デバイスの安全性レベルに応じて、いずれのベース鍵を用いるかを選択する。

MDMベース鍵リストエントリは、以下を含む。

MDMエントリ：

baseKey：int16

ベース鍵リストは、鍵セット識別子によりインデックスを付けられる。

MDMは、DUKPTベース鍵のメモリ内リストを維持する。各鍵は、112ビットを必要とする。MDMは、1024鍵を２組必要とし、合計32KBを必要とする。MDMは、他のいずれのDPCコンポーネントにも直接依存しない。

PICグループリスト

PICグループリスト(PGL)は、インディビジュアルバイオメトリックデータベースマシンリストと共に、IBDマシンの構成を定義する。PGLは、PICの管理を簡素化するために用いられるシステム内にPICグループのリストを格納する。PICグループは、一連の連続したPICコードである。PGLは、各GMマシン(GM)上に存在する。

PGLは、PICコードを与えられると、上記PICコードを含むグループを見つけるためにPICグループのリストをサーチする。PGLはグループのリストを順序立てて維持し、正しいグループを迅速に見つけるためにバイナリサーチを用いる。

PGLの初期構成は、全ての可能性のあるPICを含む１つの巨大なPICグループである。PICの閾値ナンバが割り当てられた後、巨大なPICグループは２つに分割される。その後、このプロセスが全てのPICグループに適用される。

PICグループが分割されると、PGLは、早いものからサーブする(first-come-first serve)様式で入手可能な記憶容量に基づいて、新しいメインおよびバックアップIBDマシンを割り当てる。PGLは、IBDマシンと協力して、まず、影響を受ける記録を古いメインおよびバックアップマシンから新しいものにコピーし、IML記録を更新し、最後に古いメインおよびバックアップコピーを除去する。PICグループを分割することは、複雑なタスクである。PGLバッチは、DPCのロードが軽いとき、例えば夜に実行されるように、要求を分割する。

システム管理者はさらに、マシンのフリーな記憶容量が予測された量の新しい登録を取り扱うために要するレベルを下回る場合、与えられたPICグループ用のメインおよびバックアップIBDマシンを変更し得る。

PICグループ記録用のスキーマは以下の通りである。

PICグループ：

lowPin=int8

highPin=int8

used=int4

各PICグループは、固有の識別子により識別される。便宜上、PICグループ識別コードをグループ用のlowPinコードとするが、そうでない場合システムはこの事実に依存しない。PGLはlowPinフィールドにより鍵をかけられる。

PGLグループは、約3000グループを含むと予測される（各PICグループは約1000のアクティブなPICを含むが、数百万の実際のPICをカバーし得る）。PGL全体は、約72KBの記憶容量を要し、メモリ内で完全にキャッシュされる。

PICグループが追加、マージ、または分割されると、PGLはIBDマシンリストに変更を通知し且つ１つのIBDマシンから別のIBDマシンへのIBD記録の移動を指示する責任がある。

インディビジュアルバイオメトリックデータベースマシンリスト

IBDマシンリスト(IML)は、PICグループリストと共に、IBDマシンの構成を分類する。IMLは、PICコードを、PIC用のIBD記録を格納するメインおよびバックアップIBDマシンにマッピングする。IMLは実際、個々のPICではなくPICグループ（連続したPICコードのセット）により鍵をかけられる。なぜなら、この方が、リストを格納するために要するメモリが減少するからである。IMLは各GMマシン(GM)上に存在する。

GMがバイオメトリック識別子を必要とする要求を処理すると、GMは、バイオメトリックのPICグループにより鍵をかけられたIML記録を見つける。そうすると、GMは、バイオメトリック識別子用に用いるべきメインおよびバックアップIBDマシンを知る。

IMLリストエントリ用のスキーマは以下の通りである。

マシンペア：

pinGroup=int8

main=int2

backup=int2

IMLはpinGroupにより鍵をかけられる。

IMLは、約3000のエントリ（PICグループの数）を含むと予測される。各マシンペア記録は12バイトであって約36KBの記憶容量を要し、メモリ内に完全にキャッシュされる。IBDマシンの構成のいずれの変更もが、IMLに反映されることになる。更に、IMLは、PICグループリストが改変されるとIMLもまた更新されるように、鍵用にPICグループを用いる。

シーケンスナンバモジュール

シーケンスナンバモジュール(SNM)の主要な機能は、パケットのシーケンスナンバの有効性を証明することによりレプレイ攻撃を防ぐことである。その二次的なタスクは、遠隔DPCサイトの他のSNMにシーケンスナンバの更新を通知することにより再入力攻撃の影響を最小にすること、および有効な装置データベース内のシーケンスナンバを定期的に更新することである。SNMは、BIAハードウェア識別コードによって鍵をかけられたシーケンスナンバのメモリ内ハッシュテーブルを維持して、パケットシーケンスナンバの迅速な有効性証明を可能にする。

SNMは、与えられたハードウェア識別コードとシーケンスナンバに対する有効性証明要求をGMから受け取ると、ハッシュテーブル内のハードウェア識別コードを参照する。エントリが存在しない場合、SNMはGMに「無効はハードウェア識別コード」エラーであると応答する。

そうでない場合、SNMは、ハッシュテーブルエントリ内に格納されたシーケンスナンバに照らして与えられたシーケンスナンバをチェックする。シーケンスナンバが格納されたシーケンスナンバ以下である場合、SNMは「無効なシーケンスナンバ」エラーであると応答する。そうでない場合、SNMは、ハッシュテーブルエントリ内のシーケンスナンバを、上記与えられたシーケンスナンバに設定して、

「有効なシーケンスナンバ」メッセージであると応答する。

SNMはしばしばシーケンスナンバギャップを観察し得る。シーケンスナンバギャップは、SNMがハッシュテーブルエントリ内に格納されたシーケンスナンバよ

りも１を越えた分だけ大きいシーケンスナンバを受け取るときに起こる。換言すると、シーケンスナンバはスキップされた。

SNMは、シーケンスナンバギャップを発見すると、「有効なシーケンスナンバ」メッセージに代えて「シーケンスナンバギャップ」メッセージであるとGMに応答する。GMは、パケットを有効なものとして扱うが、また「シーケンスナンバギャップ」警告を履歴に残す。

シーケンスナンバギャップは通常、ネットワーク接続可能性が失われたとき、例えば、パケットがドロップしたり、あるいはネットワークが回復して作動するまで送信できないときに起こる。しかし、シーケンスナンバギャップは、詐欺的な理由によっても起こる。悪意のある者が、パケットを傍受してDPCに到着することを妨げること、あるいは、パケットを偽造することさえあり得る（すぐに拒否されないように大きなシーケンスナンバで）。

SNMの二次的機能は、更新されたシーケンスナンバを他のDPCに通知することである。すべてのDPCサイトにおいてシーケンスナンバを迅速に更新することは、悪意のある者が１つのDPCサイトに向けられたパケットをモニタして、１つのDPCサイトから別のDPCサイトへのシーケンスナンバ更新の送信遅延を利用することを期待して即刻異なるDPCサイトにコピーを送り、その結果、第１のサイトのみがパケットを受け入れるべきときに両方のサイトがパケットを有効なものとして受け入れるという、再入力攻撃を防ぐ。

SNMは、有効なシーケンスナンバを受け取る毎に更新メッセージを互いに送信し合う。SNMは、ハッシュテーブル内に現在格納されているシーケンスナンバ以下のシーケンスナンバへの更新メッセージを受け取った場合、シーケンスナンバ再入力警告を履歴に残す。すべての再入力攻撃はこのようにして検出される。

再入力攻撃を完全に防ぐ、より簡単な方法は、１つのSNMのみにパケットの有効性を証明させることてある。このスキームの場合、再入力攻撃で利用される更新遅延ウィンドウはない。あるいは、同一のBIA搭載デバイス用のシーケンスナンバの有効性の証明を取り扱うSNMがない場合、複数のSNMが同時にアクティブになり得る。

SNMは、ブートアップすると、VAD内に格納されたアクティブなBIA用のシーケンスナンバから、シーケンスナンバハッシュテーブルをロードする。SNMは、１日に１度、現在のシーケンスナンバを、ローカルな有効装置データベース(VAD)にダウンロードする。

VADは、SNMハッシュテーブルを最新の状態に維持するためにアクティベートまたはディアクティベートされるいずれのBIA搭載デバイスに対しても、エントリ追加およびエントリ除去メッセージをSNMに送信する責任を有する。

SNMハッシュテーブルエントリは、以下を含む。

SNMエントリ：

hardwareID=int4

sequenceNumber=int4

ハッシュテーブルは、hardwareIDによって鍵をかけられる。

約500万のBIA搭載デバイスがサービスを行っているとすると、約40MBのハッシュテーブルが必要である。

SNMは、有効な装置データベースに依存する。装置が一時使用不可能にされるかデータベースから除去されると、SNMは対応するエントリを除去する。装置がアクティベートされると、SNMはそのためのエントリを作成する。

SNMは、１秒あたり1000の更新シーケンスナンバメッセージを処理するために１秒あたり約8KBの送信帯域幅を必要とする。更新シーケンスナンバメッセージは、実際に送られるメッセージの数を最小にするために、バッファに保持されて１秒に１度送出される。

発行者データベース

発行者データベース（ＩＤ）は、システムを通じてその資産アカウントへのアクセスが許される銀行及び他の金融機関についての情報を格納している。発行機関は、資産アカウント番号を、与えられた個人のＩＢＤ記録に追加したりそこから除去したりできる、唯一の存在である。

ＤＰＣは、ＩＤを使用して、発行者ターミナルの発行者コードを含む記録を求めてＩＤをサーチすることによって、発行者ターミナルからのリクエストの有効

性を検査する。記録に格納された所有者の識別子は、発行者ターミナルに記録されたＢＩＡのための有効装置データベースに格納された所有者と、一致しなければならない。

発行者記録のためのスキーマは、

発行者記録：

issuerCode＝int6

ownerId＝int4

name＝char50

phoneNumber＝char12

address＝char50

zipCode＝char9

である。

発行者データベースは、issuerCodeによって鍵をかけられる。

発行者データベースは、約100,000のエントリィを取り扱う。各々のエントリは、２ＭＢより少なく要求する127バイトである。ＩＤのコピーが、各々のＧＭに格納される。

発行者データベースは、他の何れのＤＰＣコンポーネントにも、直接の依存性を有さない。

電子文書データベース

電子文書データベース（ＥＤＤ）は、特定の個人に向けられたファックスイメージや電子メールメッセージのような電子文書を格納し、且つトラックする。それはまた、会社組織のチャートを維持して、送り手及び受け手の両方の公式な肩書きを提供する。ＥＤＤはまた、送り手或いは受け手のリクエストに応じて文書をアーカイブし、システムを通じて提出された契約同意事項に、中立の第３者の検証を与える。

ＤＰＣは、個人からファックス或いは他の電子文書を受領すると、ＥＤＤ文書

記録を生成して、承認された受け手によってピックアップされるまで、その文書を格納する。

ファックス文書に関しては、受け手は、ファックス番号及び内線によって特定される。他の電子文書に関しては、受け手は、電子メールアドレスによって特定される。ＤＰＣは、ファックス番号及び内線或いはｅメールアドレスによって個々の受け手を求めて、組織記録を調べる。もし、記録が発見されないと、ＤＰＣは次に、受け手がｅメールアドレスによって特定されるときにのみ、個人バイオメトリック記録を見る。個々の受け手に関して、ＤＰＣは、文書、及び、もし発見された場合には組織或いはＩＢＤ記録によって特定された受け手のバイオメトリック識別子、の両方を参照する受け手記録を生成する。ＤＰＣは、システムに登録されていない受け手を許容するが、そのときにはＤＰＣは、これらの受け手に対する配達或いは機密性を保証できない。

ＥＤＤは、十分にフレキシブルであって、ファックス文書が個人のｅメールアドレスに送られたり、ｅメールメッセージがファックス番号に送られることを、許容する。

文書上にシステムによって電子署名が置かれていない間は、システムは、証明されたＥメール或いはセキュリティファックスターミナルによって受領（或いは復号）されたメッセージが個人によって送られたことを、暗号化を通じて保証する。

組織の正式に承認されたオフィサーは、ＤＰＣへのファックス或いは電子メッセージへの肩書きの割り当て及びファックス番号への内線の割り当て、メンバの肩書きやファックス番号の更新、或いは、いなくなったメンバの削除、を確実に行う。

個人が組織のツリーから削除されると、ＤＰＣは、内線番号を１年間引き上げる。この引き上げ期間は、その内線番号でのコンフィデンシャルファックスを彼がもはや受領することができず、従って、その内線において、彼或いは彼女を意図していないファックスを受領し得る可能性がある他の誰かを組織が誤ってアクティベートすることがない旨を、コンフィダントに伝えるための個別の十分な時間を許容する。

ＥＤＤは、文書の送り手或いは受け手の一人によってリクエストされたときに

、文書及び受け手記録のコピーを含むアーカイブデータベースを維持する。アーカイブデータベースは、ＣＤ－ＲＯＭの上に定期的に移動される。

ＥＤＤは、３つの記録タイプを有する：

文書記録：

documentNumber＝int8

senderId＝int4

documentFax＝fax

documentText＝text

messageKey＝int8

status＝int1

受け手記録：

documentNumber＝int8

recipientId＝int4

recipientFaxNumber＝char12

recipientFaxExtension＝char8

recipientEmailAddr＝text

receivedBy＝int4

lastModified＝time

deliveryStatus＝int1

contactStatus＝int1

アーカイブリクエスト記録：

biometricId＝int4

documentNumber＝int8

requestorFaxNumber＝char12

requestorFaxExtension＝char8

requestorEmailAddr＝text

組織記録：

biometricId＝int4

registeredBy＝int4

company＝text

title＝text

faxNumber＝char12

faxExtension＝char8

emailAddr＝text

activeDate＝time

priv＝int2

status＝int1

文書記録ステータスフィールドは、

０：incomplete

１：ok

の一つである。

受け手記録デリバリステータスフィールドは、

０：incomplete

１：notified

２：rejected

３：retrieved

４：retrieved unsecured

５：busy

の一つである。

受け手記録コントラクトステータスフィールドは、

０：none

１：accepted

２：rejected

の一つである。

組織記録ステータスフィールドは、

０：active

１：suspended

の一つである。

組織記録privsフィールドは、ＤＰＣがその個人にどの特権を許容するかを示すために使用される。

０：registration

文書、受け手、及びアーカイブ取り出し記録は、documentNumberによって鍵をかけられる。組織記録は、biometricIdによって鍵をかけられる。ＥＤＤは、文書のsenderIdフィールド、受け手のrecipientIdフィールド、及び組織の会社名及び肩書きフィールドに、副インデックスを維持する。

ＥＤＤのストレジ要求は、主として、それが格納しなければならないファックスのページ数に依存する。なぜなら、ｅメールメッセージは、ファックスページに比べて比較的に小さいからである。各々のファックスページは、約１１０ＫＢのストレジを必要とする。１つのファックス毎に４ページ、一人一日当たり２つのファックスであって、３千万台のファックス機があるとすれば、ＥＤＤは、１日分のファックスをスプールするために、２４ＧＢのストレジを必要とする。

文書は、ＢＩＡ暗号化メカニズムを使用して、暗号化されたシステムへ、及びそこから、送られる。しかし、暗号化の鍵は、文書と同じデータベースに格納されている。文書は、偶然の開示を防ぐために、暗号化された形式で残される。しかし、システムに格納された文書のセキュリティに関心がある個人は、付加的な暗号化それ自身のために、何らかのアレンジメントを行う。

各々のファックスページは約１１０ＫＢを必要とし、そのことは、1.54MBits／秒のスループットを有するＴ１接続が、１秒当たり1.75ファックスページを取り扱えることを意味している。

電子署名データベース

電子署名データベースは、システムによって生成された全ての電子署名を認証してトラックする。

システムのメンバである個人は、バイオメトリックＰＩＣとともに文書に関する１６バイトの「メッセージダイジェスト」を提出して、永久にシステムにおけ

るファイル上に残る「デジタル署名」を得る。このデジタル署名は、個人の名前、バイオメトリック識別子、承認された署名記録番号、文書のタイトルを、文書が署名された時刻印とともにコード化する。

署名を検証するために、文書に関するメッセージダイジェストが（例えばＲＳＡのＭＤＳを使用して）最初に計算されて、文書の署名タグと共に送られる。ＥＳＤは、署名タグを調べて、データベースに格納されたメッセージダイジェストに対して、つい最近計算されたメッセージダイジェストの有効性を検査する。

電子署名のためのスキーマは、

電子署名：

signatureNumber＝int8

signer＝int4

documentName＝text

checksum＝int16

date＝time

である。

署名者は、文書に署名する個人に対するバイオメトリック識別コードである。電子署名記録は、signatureNumberによってハッシュされる。

１ＧＢの副ストレジ毎に、電子署名データベースは、2700万の記録（各記録は約３２バイト）を格納する。

ＥＳＤは、署名者のバイオメトリック識別子に対する依存性を有する。これらの署名は、本質的に永久に有効であるので、ＥＳＤ記録は、システムが署名者の個人バイオメトリック記録を削除するときに、除去されない。これは、ＩＢＤがバイオメトリック識別子を決して再利用しないことを必要とする旨に、留意されたい。

リモートマーチャントデータベース

リモートマーチャントデータベース（ＲＭＤ）は、電話、ケーブルテレビネットワーク、或いはインターネットを通じて商品やサービスを提供するマーチャントに関する情報を格納する。適切に備えられたターミナルを使用して個人によっ

て送られた各オーダは、マーチャントのオーダターミナルを通じてシステムにルートされる。

個人のリモートトランザクションの承認がＤＰＣによって受領され、且つＭＡＣの有効性が検査されると、マーチャントコードがＲＭＤのマーチャントコードと比較される。マーチャントコードは、それが電話番号、マーチャント－製品クレデンシャル、或いはインターネットアドレスであれば、ＲＭＤ記録の中において、正しいマーチャント識別コードの下に存在し、そうでなければ、ＤＰＣターミナルがリクエストを終了して、無効なマーチャントコードエラーを送り手のＢＩＡターミナルデバイスに送り返す。

リモートマーチャント記録のためのスキーマは、

リモートマーチャント：

merchantId＝int4

merchantCode＝char16

merchantType＝int1

publicKey＝int16

である。

リモートマーチャントのmerchantTypeは、

０：telephone

１：ＣＡＴＶ

２：Internet

の一つである。

merchantId及びmerchantCodeは、どちらも主要な鍵である。２つのＲＭＤ記録が同じmerchantId及びmerchantCodeの組合せを有することはない。

約100,000のリモートマーチャントが存在するとすれば、ＲＭＤは、必要とされる約2.4ＭＢのストレジの総量のために、１記録当たり約２４バイトを必要とする。ＲＭＤは、他のＤＰＣコンポーネントの何れに対しても直接の依存性を有さない。

システムのパフォーマンス

鍵となるパフォーマンス数は、ＤＰＣが１秒当たりいくつの金融承認トランザクションを取り扱えるかである。

ＧＭにおいて：

１．ＭＡＣＭがＭＡＣをチェックする（ローカル）

２．ＳＮＭがシーケンス番号をチェックする（ネットワークメッセージ）

３．ＭＤＭがバイオメトリック－ＰＩＣブロックを復号する（ローカル）

４．ＩＢＤマシンを見つける（ローカル）

５．識別リクエストをＩＢＤマシンに送る（ネットワークメッセージ）

ＩＢＤマシンにおいて：

６．ＰＩＣのための全てのＩＢＤ記録を取り出す（ｘがバイオメトリック記録を格納するために必要とされるページ数であるときに、ｘ回のシーク及びｘ回の読み出し）

７．各記録毎に、その主バイオメトリックに対して比較する（ｙが取り出された記録数であるときに、ｙ／２ｍｓ）

８．適切なマッチングがなければ、ステップ９を繰り返すが、副バイオメトリックに対して比較する（ｙが取り出された記録数であり、ｚがマッチングが発見されない確率であるときに、ｚ×ｙ／２ｍｓ）

９．ベストマッチングのＩＢＤ記録のチェックサム列を更新して、可能性のあるリプレイアタックをチェックする（１回のシーク、１回の読み出し、及び１回の書き込み）

１０．ベストマッチングのＩＢＤ記録、或いはみしマッチングが十分に近くないときにはエラーを、戻す（ネットワークメッセージ）

ＧＭにおいて：

１１．外部プロセッサでリクエストを承認する（ネットワークメッセージ）

１２．ＧＭがレスポンスを暗号化してＭＡＣする（ローカル）

１３．レスポンスパケットを送り返す（ネットワークメッセージ）

全ディスクコスト：

ｘ×（ｓ＋ｒ）＋ｙ／２×（１＋ｚ）＋ｓ＋ｒ＋ｗ＋５×ｎ

＝（x ＋ 1）×　s（＋）r　y＋　×　2（　　1）＋　z　　＋5×w ＋　　n

（1　[xが　２０、あ りy、ハ　カ　3　の あ、ハ　°カ、あ5り て—　　s　1—0　m　s　r

s、　w＝　0　m、s＝0 m　s　あ　る と　す れ は

＝2　1×　1　0　m　s　×＋　10 55　ml s

＝2　2　6sm

＝4．　4　T　P　S

[xが　1　0 あ、りy　ハ　カ　1あ 5り 、ハ　カ%z5　/あ　す—、　　s　1—0　m　$0 mr

s、　w＝　0　m、s＝ m　s、0てあ ると　す れ は

＝1　1×　1　0　m　s　＋×7　0　5 m 1s．

＝1　1　8sm

＝8．　4　T　P　S

[x　カ　1あてり、y　ハ カ　、1あ り　、ハ2　カ、5、/あ—す　　s　—1　0、m 0s m　s

w＝　0　m、s　＝0n m　s あ る と　す れ は

＝2×　1　0　m　1/s ×＋　0　51m. s

＝２１ｍｓ

＝４７ＴＰＳ

バックアップＩＢＤマシンが、やはり２重に有効なＴＰＳをリクエストする。

最悪のケース（２つのマシンが使用されている）：

Individuals/PIC	ＴＰＳ
３０	８
１５	１６
1	９４

平均のケース（２０のマシンが使用されている）：

Individuals/PIC	ＴＰＳ
３０	８８
１５	１６８
1	９４０

最良のケース（４０のマシンが使用されている）：

Individuals/PIC	ＴＰＳ
３０	１７６
１５	３３６
１	１８８０

上記は、商業的に存立し得る方法によって実行可能なシステムのある構成の、単なる一例である。しかし、本発明が、より速いコンピュータ、より多くのコンピュータ、及び他のそのような変化を盛り込み得る他の多くの方法によって構成され得ることが、期待される。

ターミナルプロトコルフローチャート

以下のプロトコルフローのセットは、特定のターミナル、ＤＰＣ、付属されたＢＩＡ、及びクレジット／デビットプロセッサなどの他の関係者の間でのやりとりを記述する。

小売ＰＯＳターミナル

この場合、ＲＰＴターミナルは、小売ＢＩＡ及びＤＰＣと通信して、トランザクションを承認する。トランザクション量は452.33であって、個人のアカウントは4024-2256-5521-1212であって、マーチャントコードは123456であって、個人のプライベートコードは「私はそれを完全に確信している」である。

RPT → BIA set Language　〈英語〉

BIA → RPT Ok

RPT → BIA Get Biometric　〈２０〉

BIA/LCD:　〈明るくされたパネルに指を置いて下さい〉

個人がスキャナに指を置く

BIA → RPT Ok

RPT → BIA Get Pin　〈４０〉

BIA/LCD:　〈あなたのＰＩＣを入力し、その後に〈enter〉を押して下さい〉

個人がＰＩＣを入力し、その後に〈enter〉する

BIA → RPT Ok

RPT → BIA Get Account Number　〈４０〉

BIA/LCD:　〈あなたのアカウントインデックスコードを入力し、その後に〈enter〉を押して下さい〉

個人がコードを入力し、その後に〈enter〉する

BIA → RPT Ok

RPT → BIA Validate Amount　〈452.33〉〈４０〉

BIA/LCD:　〈452.33という量はＯＫ？〉

個人がＯＫを入力する

BIA → RPT Ok

装置オーナーデータベース

装置オーナーデータベース（ＡＯＤ）は、ＢＩＡ－装備の装置を所有する個人または組織の情報を蓄積する。この情報は、金融上の貸方と借方のトランザクションのための資産アカウント情報を提供し、そして特定な個人または組織が所有する全てのＢＩＡの識別を可能にするために、ＢＩＡ装置は正当なオーナーによってのみ使用さるということの、２重のチェックを行うために使用される。

ＤＰＣが、オーナーのＢＩＡ－装備の装置の１つにより寄託される金融上のトランザクションを処理する時、各々のＡＯＤレコードは、オーナーの貸方と借方の資産アカウントを含む。例えば、販売拠点の小売り地点に取り付けられたＢＩＡから寄託されたトランザクションは、資産アカウントに対する貸方を含み、一方、認可された電子郵便トランザクションは資産アカウントの借方となる。

装置オーナーのレコードの概要は

装置のオーナー：

ownerId＝int４

name＝char５０

address＝char５０

ZipCode＝char９

assetAccont＝char１６

status＝int１

ステータス領域の１つは：

０：停止

１：動作

装置オーナーデータベースは、オーナーＩｄによって鍵がかかる。

ＡＯＤは、約２百万の装置オーナーレコードを記憶すると予想される。約２６０ＭＢの記憶領域を必要とする。各エントリは１３０バイトとなる。ＡＯＤは、オーナー識別コードによって鍵がかかるハッシュドファイルとして記憶される。ＡＯＤのコピーは各々のＧＭに蓄えられる。

登録がＡＯＤから削除または停止される時、これらの装置オーナーを参照するいかなる正当なデータベース装置記録も停止としてマークされる。さらに、ＭＡＣモジュールとシーケンスナンバーモジュールは停止された装置に対するそれらの登録を削除する。

正当な装置のデータベース

正当な装置のデータベース（ＶＡＤ）は、現在までに製造されたＢＩＡの全てを表す記録の集大成である。ＢＩＡが作動しているか、送信待ちか、または破壊されたとしてマークされているかの表示と共に、ＶＡＤ記録は、各ＢＩＡのためのメセージ認証コードの暗号化鍵を持っている。ＢＩＡからのメセージを復号化するためには、ＢＩＡが存在してＶＡＤ内にアクティブなレコードを持たなければならない。

製造時、各々のＢＩＡは固有の公開識別コードと固有のＭＡＣの暗号化鍵とを有し、これらは共にＢＩＡの展開の前にＶＡＤレコードに入れられる。

ＢＩＡは最初に構成される時、固有のハードェア識別コードを与えられる。ＢＩＡが使用される時、そのハードェア識別コードはシステムにおいて登録される。最初、そのオーナーもしくはＢＩＡの信用できる団体は装置オーナーデータベース（ＡＯＤ）の中に入れられる。次に、ＶＡＤレコードは、ＡＯＤ記録にポイントされ、そしてＢＩＡは、アクティブにセットされる。ＢＩＡからの要求はＤＰＣによって受け入れられる。

ＢＩＡは使用から除外される時は、非アクティブとしてマークされ、そしてＡ

ＯＤ記録へのリンクは壊される。ＢＩＡからの通信は受け入れられない。

各ＢＩＡタイプおよびモデルには、物理上のセキュリティレベルであるセキュリティレベルが割り当てられている。ＤＰＣは、そのＢＩＡからの要求を処理する時、どの種類の動作が許可されるかを判定するためにＢＩＡのセキュリティレベルを使用する。ＤＰＣは、また外部の金融トランザクション認証サービスにセキュリティレベルを提供する。

認証サービスも、リスクに基づいてトランザクションのためにどれほどチャージするかのガイドとしてセキュリティレベルを使用できる。セキュリティレベルとそれらが許可する動作は、操作において決定される。

正当な装置のレコードの概要は

正当な装置：

hardwareId＝int４

macEncryptionKey＝int１６

ownerId＝int８

mfgDate＝time

inServiceDate＝time

securityLevel＝int２

status＝int１

type＝int１

use＝int１

ステータスフィールドの可能な数値は：

０：停止

１：動作（アクティブ）

２：破壊

タイプフィールドの可能な数値は（各ターミナルタイプに対して１つ）：

０：ＡＴＭ

１：ＢＲＴ

２：ＣＥＴ

３：ＣＰＴ

４：ＣＳＴ

５：ＥＳＴ

６：ＩＰＴ

７：ＩＴ

８：ＩＴＴ

９：ＰＰＴ

１０：ＲＰＴ

１１：ＳＦＴ

使用フィールドの可能な数値は：

０：リテイル

１：個人

２：発行人

３：遠隔

正当な装置のデータベースはハードウェアの識別コードによって鍵がかかる。

ＶＡＤは約５百万のリテイル、発行人、および遠隔の正当な装置エントリを扱う。各エントリは５１バイトとなり、合計約２５５ＭＢを必要とする。ＶＡＤは、ハードウェア識別コードによって鍵がかかるハッシュドファイルとして記憶される。ＶＡＤのコピーは各ＧＭ上に記憶される。

個人的な正当な装置エントリの数は、３千万の範囲であり、１．５ＭＢの記憶領域を必要とする。

ＶＡＤレコードがステータスに変わる時、ＭＡＣモジュールおよびシーケンスナンバーモジュールは、そのステータスの変化について通知される。例えば、装置がアダプティブになると、ＭＡＣＰ及びＳＮＭは、新しくアダプティブとなった装置のエントリを追加する。装置が非アダプティブになると、ＭＡＣＰ及びＳＮＭは、その装置のエントリを削除する。

個人バイオメトリックデータベース

個人バイオメトリックデータベース（ＩＢＤ）レコードは個人の情報を記憶し

、それらは、１次的、２次的なバイオメトリック、ＰＩＣコード、金融資産アカウントのリスト、プライベートコード、緊急アカウント、アドレス、そして電話番号を含む。個人は、これらのＳＳＮと電子メールアドレスを選択的に持っている。この情報は、バイオメトックか個人情報のどちらかによって個人を識別するか、アカウントの情報にアクセスするか、または追加された検証のためアドレスまたは電話番号を遠隔のトランザクション者に提供するために必要である。

世界規模のリテイル銀行組織内で、またはローカルシステムオフィス内に位置する登録されたバイオメトリック登録ターミナルでの個人記録プロセスの間に、個人はシステムに追加される。登録の間、個人は、その個人識別ナンバーを選択

し、そして、そのバイオメトリックとＰＩＣコとの組み合わせに金融資産アカウントを追加する。

個人は、発行ナンバーによって不正活動が報告されると、データベースから削除され得る。これが起こると、認可された内部システムの代表によって、個人のアカウント情報はＩＢＤから以前の詐欺データベース（ＰＦＤ）に移動される。ＰＦＤ内のレコードにためのバイオメトリックＩｄはＩＢＤ内のレコードのために使用されない。

そのＩＢＤは、複数の装置に存在し、各々の装置は、過剰と負荷分担の両方に対して、２つの異なる装置に記憶された各レコードのコピーと共にＩＢＤレコードの下位集合に責任がある。

個人バイオメトリックレコードの概要は：

個人バイオメトリック：

primaryBiometric＝Biometric

secondaryBiometric＝Biometric

BiometricId＝int４

ＰＩＣ＝char１０

phoneNumber＝char１２

lastName＝char２４

firstName＝char２４

middleInitial＝char２

ＳＳＮ＝char９

privateCode＝char４０

address＝char５０

ZipCode＝char９

publicKey＝char６４

checksums＝int４［１０］

accontLinks＝char３０［１０］

emergencyIndex＝char１

emergencyLink＝char１

privs＝char１０

enroller＝int８

emergencyUseCount＝int４

status＝int１

ステータスフィールドは次の１つ：

０：停止

１：動作

２：以前の詐欺

ＩＢＤはＰＩＣによって鍵がかけられる。

各々のＩＢＤ装置は、ＩＢＤへのアクセスを容易にするため、個人のセキュリティナンバー、バイオメトリック識別コード、ラストネーム、ファーストネーム、そして電話番号について付加的なインデックスを持っている

各ＩＢＤ装置は１つ以上のＲＡＩＤデバイスによって提供される４０ＭＢの２次記憶装置を持っている。各々のＩＢＤレコードは、バイオメトリックが各々１Ｋと仮定すると２６５８バイトであり、装置あたり１５百万レコードまで可能である。ＩＢＤレコードは、ＰＩＣ上の（おそらく群状の）２次インデックスを使って記憶される。インデックスはメモリーに記憶され、６４ＭＢ（６４ＭＢインデックスは約１６百万のエントリを扱う）しか必要としない。３億の個人のため

のレコードを記憶するためには、ＤＰＣは、少なくとも４０のＩＢＤ装置が、主記憶装置として２０個のＩＢＤ装置およびバックアップとしてさらに２０個が必要となる。

ＩＢＤ装置の数は、登録される個人の数によって容易に増減される。

ＩＢＤ装置、ＰＩＣグループリスト、そしてＩＢＤ装置リストは、どのＰＩＣがどの装置上のあるのかによって、最新のもので残される。ＰＩＣグループが再構成されるか、またはＰＩＣグループのメインとバックアップが変わる時、ＩＢＤ装置は、これらのデータベースとインデックスを適切に更新する。

承認された個人データベース

各々の発行人または個人のＢＩＡ装備デバイスに対して、認可された個人データベース（ＡＩＤ）は、デバイスのオーナーによって使用が承認された個人のリストを保持する。

ＡＩＤは次の２つの理由にために存在する。その第一理由はターミナルに限されたアクセスを提供することである。例えば、発行人のターミナルは、承認された銀行の代表によってのみ使用され得る。ＡＩＤの第２の理由は、犯罪者が電話ターミナルの個人のＢＩＡに秘密裏に置き換え、リテイルＰＯＳターミナルのＢＩＡを販売拠点のリテイル点において、すべての購入物を犯罪者によって設定された遠隔のトランザクション者のアカウントに仕向けるのを防ぐことである。

承認された個人のレコードの概要は：

承認された個人：

hardwareId＝int 4

biometricId＝int 4

HardwareＩｄは、正当な装置のデータベースにおけるレコードを意味し、そしてbiometricＩｄは、個人のバイオメトリックデータベースを意味する。

ＤＰＣは、個人が個人または発行人ＢＩＡデバイスを利用することが承認されるかどうかのチェックが必要なときはいつでも、ＤＰＣは、正しいHardwareＩｄとbiometricＩｄとを持つ承認された個人レコードの存在をチェックする。

個人ＢＩＡデバイスは、正当な装置のデータベースにおいて１（個人）に設定

された使用フィールドによって識別される。発行人ＢＩＡデバイスは正当な装置のデータベースにおいて２（発行人）に設定された使用フィールドによって識別される。

各発行人のターミナルは、それを使うことが承認された１０の個人を持ち、各個人デバイスが、２つの追加の承認された個人を持ち、サーバ内には１，０００，０００の個人デバイスがあるとすると、ＡＩＤの蓄積は：

１０×１００，０００＋２×１，０００，０００－３，０００，０００エントリ

を記憶する。データベース全体は約２４ＭＢの記憶領域を必要とする。

承認されたオーナーデーターベースレコードまたは正当な装置データベースレコードが削除される時、それらを参照している全ての承認された個人レコードが削除される。

以前の詐欺のデータベース

以前の詐欺のデータベース（ＰＦＤ）は、過去におけるある時点でだまされたメンバー発行人を持つ個人を表わすレコードの集大成である。ＰＦＤはまた、ＰＦＤ内に一致した記録を持つＩＢＤ内の個人を除去するため、低いシステム動作期間の間、背景のトランザクションを走らせる。

個人が再度登録を試みていることを検出しない限り、システムは、自動的に個人をＰＦＤ内に入れることはない。個人をＰＦＤに置くことは、本明細書の範囲外の微妙な施策事項である。

新しいＩＢＤレコードがアクティブであるとしてマークされる前に、個人の１次的そして２次的なバイオメトリックスは、個人の識別手続きで使用されるものと同じバイオメトリック比較技術を用いてＰＦＤにおける各々のそして全てのバイオメトリックに対してチェックされる。新しいＩＢＤレコードに一致が見つかると、ＩＢＤレコードのステータスは「以前の詐欺」に設定される。以前の詐欺のチェックが、登録要求の一部として実行される場合は、ＧＭは「以前の詐欺を持つ個人を登録中」という警告を出す。

ＰＦＤは、比較的小さいままであると仮定する。自発的でないバイオメトリックサーチのため、ＰＦＤを動かすコストは、高い。

以前の詐欺レコードの概要は：

以前の詐欺：

primaryBiometric＝Biometric

secondaryBiometric＝Biometric

BiometricId＝int４

ＰＩＣ＝char１０

phoneNumber＝char１２

lastName＝char２４

firstName＝char２４

middleInitial＝char２

ＳＳＮ＝char９

privateSignal＝char４０

address＝char５０

ZipCode＝char９

publicKey＝char６４

checksums＝int４［１０］

accontLinks＝char３０［１０］

emergencyIndex＝char１

emergencyLink＝char１

privs＝char１０

enroller＝int８

emergencyUseCount＝int４

status＝int１

ステータス領域は次の１つ：

０：停止

１：動作（アクティブ）

２：以前の詐欺

ＰＦＤは、バイオメトリック識別コードによって鍵をかけられる。

ＰＦＤレコードは、ＩＢＤレコードと同じである。幸運にも、ＤＰＣは、これらのほんの僅かしか記憶する必要がないため、データベース全体を記憶するためには２つのデータベース装置が必要なだけである。これらの内、１つはバックアップである。ＰＦＤは、他のいずれのＤＰＣ構成要素にも直接依存しない。

ＲＰＴ→ＢＩＡ　レジスタを割り当てよ　〈1〉〈１２３４５６〉

ＢＩＡ→ＲＰＴ　ＯＫ

ＲＰＴ→メッセージを形成〈トランザクション〉

ＢＩＡ→ＲＰＴ　〈トランザクションリクエストメッセージ〉

ＢＩＡ→ＲＰＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＲＰＴ→ＤＰＣ　〈トランザクションリクエストメッセージ〉

ＤＰＣ：バイオメトリックの有効性証明、アカウント番号取り出し

→４０２４－２２５６－５５２１－１２１２

ＤＰＣ→ＶＩＳＡ　〈承認　４０２４－２２５６－５５２１－１２１２　４５２．３３　１２３４５６〉

ＶＩＳＡ→ＤＰＣ　〈ＯＫ　４０２４－２２５６－５５２１－１２１２　４５２．３３　１２３４５６　承認コード〉

ＤＰＣ：秘密コード取得

ＤＰＣ→ＲＰＴ　〈トランザクションレスポンスメッセージ〉

ＲＰＴ→ＢＩＡ　レスポンスを示せ〈トランザクションレスポンスメッセージ〉〈8〉

ＢＩＡ／ＬＣＤ：〈トランザクション　ＯＫ：Ｉ am fully persuad　　ed of it〉

ＢＩＡ→ＲＰＴ　〈ＯＫ〈承認コード〉〉

ＲＰＴ：承認コードをレシートに印刷せよ

インターネットＰＯＳ端末（Internet Point of Sale Terminal）

この場合、ＩＰＴはトランザクションの承認のため標準ＢＩＡ、ＤＰＣと通信する。トランザクション量は４５２．３３、個人アカウントは４０２４－２２５

６－５５２１－１２１２、インターネット商人はｍｅｒｃｈａｎｔ．ｃｏｍに位置し、その商人コードは１２３４５６、そして個人の秘密コードは「Ｉ am fully persuaded of it.」である。

ＩＰＴ→ｍｅｒｃｈａｎｔ．ｃｏｍ　〈リソースが使用可能であれば商人コードを私に送れ〉

ｍｅｒｃｈａｎｔ．ｃｏｍ→ＩＰＴ　〈ＯＫ　１２３４５６　ｍｅｒｃｈａｎｔ．ｃｏ　ｍ公開鍵〉

ＩＰＴはセッション鍵を生成し、ｍｅｒｃｈａｎｔ．ｃｏｍ公開鍵で暗号化

ＩＰＴ→ｍｅｒｃｈａｎｔ．ｃｏｍ　〈セッション鍵〉

商人との全てのその後の通信はセッション鍵で暗号化

ｍｅｒｃｈａｎｔ．ｃｏｍ→ＩＰＴ　〈価格及び製品情報〉

ＩＰＴ／スクリーン：価格及び製品情報を表示

個人：「フルーツケーキ、価格４５．３３」の項目を選択

ＩＰＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ－ＢＩＡ　バイオメトリックを取得せよ〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　アカウント番号を取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈今度はあなたのアカウントインデックスコードを入力し、その後〈入力〉を押して下さい。〉

個人はコードを入力し、その後〈入力〉を押す。

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　量の有効性を証明せよ〈４５．３３　　〉〈４０〉

ＢＩＡ／ＬＣＤ：〈量４５．３３　ＯＫ？〉

個人はＯＫを入力する

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈１２３４５６〉

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　レジスタを割り当てよ　〈２〉〈ｍｅｒｃｈａｎｔ．ｃｏｍ〉

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　レジスタを割り当てよ　〈３〉〈フルーツケーキ〉

ＢＩＡ→ＩＰＴ　ＯＫ

ＩＰＴ→ＢＩＡ　メッセージ形成　〈遠隔トランザクション〉

ＢＩＡ→ＩＰＴ　〈遠隔トランザクションリクエストメッセージ〉

ＢＩＡ→ＩＰＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＩＰＴ→ｍｅｒｃｈａｎｔ．ｃｏｍ　〈遠隔トランザクションリクエストメッセージ〉

ｍｅｒｃｈａｎｔ．ｃｏｍ→ＤＰＣ公開鍵を用いてＤＰＣと安全接続

ｍｅｒｃｈａｎｔ．ｃｏｍ→ＤＰＣ　〈遠隔トランザクションリクエストメッセージ〉

ＤＰＣ：バイオメトリックの有効性証明、アカウント番号取り出し

→４０２４－２２５６－５５２１－１２１２

ＤＰＣ：コード１２３４５６によりインターネットｍｅｒｃｈａｎｔ．ｃｏｍの有効性証明

ＤＰＣ→ＶＩＳＡ　〈承認　４０２４－２２５６－５５２１－１２１２

４５．３３　１２３４５６〉

ＶＩＳＡ→ＤＰＣ　〈　ＯＫ　４０２４－２２５６－５５２１－１２１２　４５．３３　１２３４５６　承認コード〉

ＤＰＣ：秘密コードを取得

ＤＰＣ→ｍｅｒｃｈａｎｔ．ｃｏｍ〈トランザクションレスポンスメッセージ〉

ｍｅｒｃｈａｎｔ．ｃｏｍは承認コードを格納

ｍｅｒｃｈａｎｔ．ｃｏｍ→ＩＰＴ〈トランザクションレスポンスメッセージ〉

ＩＰＴ→ＢＩＡ　レスポンスを示せ〈トランザクションレスポンスメッセージ〉〈８〉

ＢＩＡ／ＬＣＤ：〈トランザクションＯＫ：I am fully persuaded of it〉

ＢＩＡ→ＩＰＴ〈トランザクション　ＯＫ〉

インターネット料金計算ターミナル（Internet Teller Terminal）

この場合、ＩＴＴは定型または非定型のホームバンキング操作を実行するために標準ＢＩＡ、ＤＰＣ及び銀行のインターネットサーバと通信する。ＤＰＣは実際には、トランザクションの有効性を承認することには関わらず、ネットワークレデンシャルの有効セットを作成すること及び銀行との通信回線の確保をすることについてのみ責任を負う。

ＩＴＴ→ｂａｎｋ．ｃｏｍ　〈リソースが使用可能であれば銀行コードを私に送れ〉〉

ｂａｎｋ．ｃｏｍ→ＩＴＴ〈ＯＫ　１２００〉

ＩＴＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

　ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

　個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＩＴＴ　ＯＫ

ＲＰＴ→ＢＩＡ　アカウント番号を取得せよ〈４０〉

　ＢＩＡ／ＬＣＤ：〈次にアカウントインデックスコードを入力し、そして、〈入力〉を押して下さい〉

　個人はコードを入力し、〈入力〉を押す。

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈１２００〉（銀行コード）

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→ＢＩＡ　レジスタを割り当てよ　〈２〉〈ｂａｎｋ．ｃｏｍ〉

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→ＢＩＡ　レジスタを割り当てよ　〈３〉〈ＩＴＴ．ｐｏｒｔ、ｂａｎｋ．ｃｏｍ．ｐｏｒｔ〉（ＴＣＰ／ＩＰアドレス）

ＢＩＡ→ＩＴＴ　ＯＫ

ＩＴＴ→メッセージを形成せよ　〈ネットクレデンシャル〉

ＢＩＡ→ＩＴＴ　〈ネットワーククレデンシャルリクエスト〉

ＢＩＡ→ＩＴＴ　ＯＫ

　ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＩＴＴ→ＤＰＣ　〈ネットワーククレデンシャルリクエスト〉

　ＤＰＣ：バイオメトリックの有効性証明、クレデンシャル（時間、アカウント、銀行）を生成

　ＤＰＣ：秘密コード取得

ＤＰＣ→ＩＴＴ　〈ネットワーククレデンシャルレスポンス〉

ＩＴＴ→ＢＩＡ　レスポンスを示せ　〈ネットワーククレデンシャルレスポンス〉

ＢＩＡはレスポンスを復号化し、レスポンスを検査する

ＢＩＡ／ＬＣＤ：〈クレデンシャルＯＫ：I am fully persuaded of it〉

ＢＩＡは銀行の公開鍵を用いて、クレデンシャル、セッション鍵、

チャレンジ鍵を暗号化する

ＢＩＡ→ＩＴＴ　〈安全接続リクエストメッセージ〉

ＢＩＡ→ＩＴＴ　〈セッション鍵〉

ＢＩＡ→ＩＴＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ｂａｎｋ．ｃｏｍとの安全接続中〉

ＩＴＴ→ｂａｎｋ．ｃｏｍ　〈安全接続リクエストメッセージ〉

ｂａｎｋ．ｃｏｍは秘密鍵を用いて暗号し、クレデンシャルの有効性を証明し、共用鍵を使用する。

ｂａｎｋ．ｃｏｍ→ＩＴＴ　〈ＯＫ〉

ＩＴＴ→ｂａｎｋ．ｃｏｍ接続の更なるトランザクションは全てＩＴＴ／銀行セッション鍵を用いてＩＴＴによって暗号化される。

銀行が非定型であると決定するあらゆるトランザクションは、ＢＩＡのチャレンジーレスポンス機構を用いて個人によって確認されなければならない。チャレンジーレスポンス機構は、ＢＩＡが「安全接続」状態にある場合にのみ利用可能である。

ｂａｎｋ．ｃｏｍ→ＩＴＴ　〈〈有効性証明要求〉の有効性を証明〉

ＩＴＴ→ＢＩＡ　秘密〈暗号化有効性証明要求〉の有効性を証明

ＢＩＡはチャレンジセクションを復号化し、表示する。

ＢＩＡ／ＬＣＤ：〈ＯＫです：１２，４２０．００から１０２３－３３０２－２１０１－１１００に転送〉

個人はＯＫを入力する。

ＢＩＡはチャレンジ鍵を用いてレスポンスの再暗号化をする。

ＢＩＡ／ＬＣＤ：〈ｂａｎｋ．ｃｏｍに安全接続中〉

ＢＩＡ→ＩＴＴ　〈ＯＫ〈暗号化された有効性証明レスポンス〉〉

ＩＴＴ→ｂａｎｋ．ｃｏｍ　〈暗号化された有効性証明レスポンス〉

電子署名端末（Electronic Signature Terminal）

この場合、ＥＳＴはディジタル署名を作成するため、標準ＢＩＡ及びＤＰＣと通信する。個人の秘密コードは「I am fully persuaded of it.」であり、署名される文書は「The Letter of Marque.」と呼ばれる。

ＣＥＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　文書の有効性を証明せよ　〈Letter of Marque〉〈４０〉

ＢＩＡ／ＬＣＤ：〈文書「Letter of Marque」　ＯＫ？〉

個人はＯＫを入力する。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈文書ＭＤ５値〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→メッセージを形成せよ　〈署名提出〉

ＢＩＡ→ＣＥＴ　〈電子署名リクエスト〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＣＥＴ→ＤＰＣ　〈電子署名リクエスト〉

ＤＰＣ：バイオメトリックの有効性を証明、署名を生成、署名テキストコードを返す

ＤＰＣ：秘密コード取得

ＤＰＣ－ＣＥＴ　〈電子署名レスポンス〉

ＣＥＴ→ＢＩＡ　レスポンスを示せ　〈電子署名レスポンス〉〈８〉

ＢＩＡ／ＬＣＤ：〈文書ＯＫ：I am fully persuaded of it.〉

ＢＩＡ→ＣＥＴ　〈ＯＫ〈署名テキストコード〉〉

認可された電子メールターミナル（Certified Email Terminal）

この場合は、ＣＥＴは認可された電子メールを送信するために、標準ＢＩＡ及びＤＰＣと通信する。個人の秘密コードは「I am fully persuaded of it.」であり、文書名は「Post Captain.」である。

ＣＥＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　文書の有効性を証明せよ　〈Post Captain〉〈４０〉

ＢＩＡ／ＬＣＤ：〈文書「Post Captain」でＯＫ？〉

個人はＯＫを入力する。

ＣＥＴ／スクリーン：　〈受け手リスト？〉

個人は〈fred@telerate.com joe@reuters.com〉を入力する。

ＣＥＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈fred@telerate.com joe@reuters.com〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→メッセージを形成せよ　〈文書提出〉

ＢＩＡ→ＣＥＴ　〈電子文書提出リクエスト〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＣＥＴ→ＤＰＣ　〈電子文書提出リクエスト〉

ＤＰＣ：バイオメトリックの有効性を証明、メッセージを生成、メッセージ＃００１２３４を返す。

ＤＰＣ：秘密コード取得

ＤＰＣ→ＣＥＴ　〈電子文書提出レスポンス〉

ＣＥＴ→ＢＩＡ　レスポンスを示せ　〈電子文書提出レスポンス〉〈８〉

ＢＩＡ／ＬＣＤ：〈文書ＯＫ：I am fully persuaded of it.〉

ＢＩＡ→ＣＥＴ　〈文書ＯＫ　〈１２３４〉〉

ＣＥＴ→ＤＰＣ　〈電子文書データリクエスト、１２３４、セクション１、未完〉

ＤＰＣ→ＣＥＴ　〈電子文書データレスポンス、未完〉

ＣＥＴ→ＤＰＣ　〈電子文書データリクエスト、１２３４、セクション２、未完〉

ＤＰＣ→ＣＥＴ　〈電子文書データレスポンス、未完〉

ＣＥＴ→ＤＰＣ　〈電子文書データリクエスト、１２３４、セクション３、未完〉

ＤＰＣ→ＣＥＴ　〈電子文書データレスポンス、未完〉

ＣＥＴ→ＤＰＣ　〈電子文書データリクエスト、１２３４、セクション

４、終了〉

ＤＰＣ→ＣＥＴ　〈電子文書データレスポンス、トラック１２３４．１　１２３４．２〉

ＤＰＣ→fred@telerate.com　〈ｅメール　１２３４．１　メッセージ到着〉

ＤＰＣ→joe@reuters.com　〈ｅメール　１２３４．２　メッセージ到着〉

mailer@telerate.com →ＤＰＣ　〈１２３４．１　の受理通知ｅメール〉

ＤＰＣ→sender@company.com〈ｅメール　１２３４．１　受け手に通知された〉

mailer@reuters.com→ＤＰＣ　〈１２３４．２　の受理通知ｅメール〉

ＤＰＣ→sender@company.com〈ｅメール　１２３４．２　受け手に通知された〉

［フレッドのＣＥＴでは、フレッドは「メッセージ到着」の電子メールメッセージを見て、すぐにそのメッセージを採用することを決める］

ＣＥＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉　ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力しして下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→ＢＩＡ　レジスタを割り当てよ　〈1〉〈１２３４．１〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＣＥＴ→メッセージを形成せよ　〈文書取り出し〉

ＢＩＡ→ＣＥＴ　〈電子文書取り出しリクエスト〉

ＢＩＡ→ＣＥＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＣＥＴ→ＤＰＣ　〈電子文書取り出しリクエスト〉

ＤＰＣ：バイオメトリックの有効性証明、１２３４．１の検索

ＤＰＣ：秘密コード取得

ＤＰＣ→ＣＥＴ　〈電子文書取り出しレスポンス〉

ＣＥＴ→ＢＩＡ　レスポンスを示せ　〈電子文書取り出しレスポンス〉〈8〉

ＢＩＡ／ＬＣＤ：〈文書ＯＫ：I am fully persuaded of it.〉

ＢＩＡ→ＣＥＴ　〈文書ＯＫ　〈メッセージ鍵〉〉

ＣＥＴ／スクリーン：復号化し、その後文書表示

安全ファックス端末（Secure Fax Terminal）

この場合、ＳＦＴは安全なファックスを送信するため、ＢＩＡ／ｃａｔｖ及びＤＰＣと通信する。

ＳＦＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＳＦＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＳＦＴ→ＢＩＡ　ＰＩＮを設定せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのタイトルインデックスを入力し、その後〈入力〉を押して下さい。〉

個人はタイトルインデックスを入力し、その後〈入力〉を押す。

ＳＦＴ→ＢＩＡ　タイトルインデックスコードを設定せよ　〈４０〉

ＢＩＡ→ＳＦＴ　ＯＫ

ＳＦＴ／スクリーン：　〈受け手？（内線は＊を追加して、最後に＃を付ける）〉

個人は〈１　５１０　９４４－６３００＊５２５＃〉を入力

ＳＦＴ／スクリーン：　〈受け手？（内線は＊を追加して、最後に＃を付ける）〉

個人は〈１　４１５－８７７－７７７０＃〉を入力

ＳＦＴ／スクリーン：　〈受け手？（内線は＊を追加して、最後に＃を付ける）〉

個人は〈＃〉を入力

ＳＦＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈１５１０９４４６３００＊５２５　１４１５８７７７７７０〉

ＢＩＡ→ＳＦＴ　ＯＫ

ＳＦＴ－メッセージを形成せよ　〈文書提出〉

ＢＩＡ→ＳＦＴ　〈安全ファックス提出リクエスト〉

ＢＩＡ→ＳＦＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＳＦＴ→ＤＰＣ　〈安全ファックス提出リクエスト〉

ＤＰＣ：バイオメトリックの有効性証明、メッセージを生成、メッセージ＃００１２３４を返す。

ＤＰＣ：秘密コード取得

ＤＰＣ→ＳＦＴ　〈安全ファックス提出レスポンス〉

ＳＦＴ→ＢＩＡ　レスポンスを示せ〈安全ファックス提出レスポンス〉〈１０〉

ＢＩＡ／ＬＣＤ：〈文書ＯＫ：I am fully persuaded of it.〉

ＢＩＡ→ＳＦＴ　〈文書ＯＫ　〈００１２３４〉〉

ＳＦＴ→ＤＰＣ　〈安全ファックスデータリクエスト、１２３４、セクション　１、未完〉

ＤＰＣ→ＳＦＴ　〈安全ファックスデータレスポンス、未完〉

ＳＦＴ→ＤＰＣ　〈安全ファックスデータリクエスト、１２３４、セクション　２、未完〉

ＤＰＣ→ＳＦＴ　〈安全ファックスデータレスポンス、未完〉

ＳＦＴ→ＤＰＣ　〈安全ファックスデータリクエスト、１２３４、セクション　３、未完〉

ＤＰＣ→ＳＦＴ　〈安全ファックスデータレスポンス、未完〉

ＳＦＴ→ＤＰＣ　〈安全ファックスデータリクエスト、１２３４、セクション　４、終了〉

ＤＰＣ→ＳＦＴ　〈安全ファックスデータレスポンス〉

ＤＰＣ→ファックス接続　１５１０９４４６３００

ＤＰＣ→ＳＦＴ６３００　〈ファックスの表紙　「Sam Spade」　「Fred Jones」より　１２３４．１　４ページ待ち〉

ＤＰＣ→接続切断

ＤＰＣ→ファックス接続　１４１５８７７７７７０

ＤＰＣ→ＳＦＴ７７００　〈ファックスの表紙　「John Jett」　「Fred Jones」より　１２３４．２　４ページ待ち〉

ＤＰＣ→接続切断

［サムのＳＦＴでは、サムはフレッドから到着した文書ファックスの表紙を見て、トラッキングコード１２３４．１を用いてＤＰＣからの文書の取り出しを開始する。］

ＳＦＴ→ＢＩＡ　バイオメトリックを取得せよ　〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人（サム）は指をスキャナーの上に置く。

ＢＩＡ→ＳＦＴ　ＯＫ

ＳＦＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＳＦＴ　ＯＫ

ＳＦＴ→ＢＩＡ　レジスタを割り当てよ　〈１〉〈１２３４．１〉

ＢＩＡ→ＳＦＴ　ＯＫ

ＳＦＴ→メッセージを形成せよ　〈文書取り出し〉

ＢＩＡ→ＳＦＴ　〈安全ファックス取り出しリクエスト〉

ＢＩＡ→ＳＦＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈ＤＰＣ本部と対話中〉

ＳＦＴ→ＤＰＣ　〈安全ファックス取り出しリクエスト〉

ＤＰＣ：バイオメトリックの有効性を証明、１２３４．１の検索、バイオメトリックＰＩＣ－Sam Spade を確認する。

ＤＰＣ：データベースの秘密コードを検索

ＤＰＣ→ＳＦＴ　〈安全ファックス取り出しレスポンス〉

ＳＦＴ→ＢＩＡ　レスポンスを示せ　〈安全ファックス取り出しレスポンス〉〈８〉

ＢＩＡ→ＳＦＴ　〈文書ＯＫ：I am fully persuaded of it　〈メッセージ鍵〉〉

ＳＦＴ／スクリーン：〈文書ＯＫ：I am fully persuaded of it〉

ＳＦＴ／スクリーン：ファックス印字

バイオメトリック登録端末（Biometric Registration Terminal）

この場合には、ＢＲＴは個人をシステムに登録するために、登録ＢＩＡおよびＤＰＣと交信する。

ＢＲＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＢＲＴ　ＯＫ

ＢＲＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉〈人差し指〉

ＢＩＡ／ＬＣＤ：〈人差し指を光っているパネルの上に置いて下さ

い。〉

個人は人差し指をスキャナーの上に置く。

ＢＩＡ→ＢＲＴ　ＯＫ

ＢＲＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉〈中指〉

ＢＩＡ／ＬＣＤ：〈中指を光っているパネルの上に置いて下さい。

〉

個人は中指をスキャナーの上に置く。

ＢＩＡ→ＢＲＴ　ＯＫ

ＢＲＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人は１２３４５６と入力し、その後〈入力〉を押す。

ＢＩＡ→ＢＲＴ　ＯＫ

ＢＲＴ→ＢＩＡ　メッセージ鍵を取得せよ

ＢＩＡ→ＢＲＴ　〈ＯＫ〈メッセージ鍵〉〉

ＢＩＡ→〈登録要求メッセージ〉

ＢＲＴ／スクリーン：〈名前：〉

代表者は入力する。〈フレッド＝Ｇ＝シュルツ（Fred G.Shultz）〉

ＢＲＴ／スクリーン：〈住所：〉

代表者は入力する。〈メイン州　北　１２３４〉

ＢＲＴ／スクリーン：〈郵便番号〉

代表者は入力する。〈９４０４２〉

ＢＲＴ／スクリーン：〈秘密コード〉

代表者は個人に照会し、その後入力する。〈私はそれを完全に信じる。（I am fully persuaded of it.）〉

ＢＲＴ／スクリーン：〈資産アカウントリスト〉

代表者は入力する。〈２，１００１－２００１－１０２０－２０１

1〉

（クレジットカード）

代表者は入力する。〈3，１００１－１００２－００３９－２２１2〉

（当座預金）

ＢＲＴ／スクリーン：〈緊急のアカウント〉

代表者は入力する。〈1，１００１－１００２－００３９－２２１2〉

（緊急、当座預金）

ＢＲＴ→メッセージを作成せよ〈登録〉

ＢＩＡ→ＢＲＴ　〈登録要求メッセージ〉

ＢＩＡ→ＢＲＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈私はＤＰＣ中央と対話している〉

ＢＲＴはメッセージ鍵により暗号化された個人情報を要求に付加する。

ＢＲＴ→ＤＰＣ　〈登録要求メッセージ〉〈暗号化された個人情報〉

ＤＰＣ：ＰＩＣ１２３４５６を検証する。

ＤＰＣ→ＢＲＴ　〈登録応答メッセージ〉

ＢＲＴ→ＢＩＡ　応答を示せ〈登録応答メッセージ〉〈8〉

ＢＩＡ／ＬＣＤ：〈登録ＯＫ：私はそれを完全に信じる。（I am fully persuaded of it.）、１２３４５６〉

ＢＩＡ→ＢＲＴ　〈ＯＫ〉

消費者サービス端末（Customer Service Terminal）

この場合には、ＣＳＴは個人の同一性およびクリデンシャルを検証するために、標準ＢＩＡおよびＤＰＣと交信する。

ＣＳＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＣＳＴ　ＯＫ

ＣＳＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＣＳＴ　ＯＫ

ＣＳＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＣＳＴ　ＯＫ

ＣＳＴ→ＢＩＡ　メッセージ鍵を取得せよ

ＢＩＡ→ＣＳＴ　〈ＯＫ〈メッセージ鍵〉〉

ＣＳＴ→メッセージを作成せよ〈個人同一性要求〉

ＢＩＡ→ＣＳＴ　〈個人同一性要求〉

ＢＩＡ→ＣＳＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈私はＤＰＣ中央と対話している〉

ＣＳＴ→ＤＰＣ　〈個人同一性要求〉

ＤＰＣ：秘密コード、すなわち個人の秘密コード（priv）を取得する。

ＤＰＣ→ＣＳＴ　〈個人同一性返答〉

ＣＳＴ→ＢＩＡ　応答を示せ〈個人同一性返答〉〈８〉

ＢＩＡ／ＬＣＤ：〈同一性ＯＫ　：私はそれを完全に信じる。（I am fully persuaded of it.）〉

ＢＩＡ→ＣＳＴ　〈ＯＫ〈個人名秘密コード（priv）〉〉

ＣＳＴ：ＣＳＴの使用にとって十分であるか知るために秘密コード（priv）を検査する。

発行者端末（Issuer Terminal）

この場合、ＩＴはアカウントの追加および削除の要求のバッチを承認し、ＤＰＣに対して送信するために、標準ＢＩＡおよびＤＰＣと交信する。個人の秘密コードは「私はそれを完全に信じる。（I am fully pursuaded of it.）」であり

、銀行コードは１２００である。

ＩＴ→ＢＩＡ　言語を設定せよ〈英語〉

ＢＩＡ→ＩＴ　ＯＫ

ＩＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉

ＢＩＡ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＩＴ　ＯＫ

ＩＴ→ＢＩＡ　ＰＩＮを取得せよ〈４０〉

ＢＩＡ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＰＩＣを入力し、その後〈入力〉を押す。

ＢＩＡ→ＩＴ　ＯＫ

ＩＴ→ＢＩＡ　レジスタを割り当てよ〈1〉〈１２００〉

ＢＩＡ→ＩＴ　ＯＫ

ＩＴ→ＢＩＡ　メッセージ鍵を取得せよ

ＢＩＡ→ＩＴ　〈メッセージ鍵〉

ＢＩＡ→ＩＴ　ＯＫ

ＩＴ→ＢＩＡ　メッセージを作成せよ〈発行者要求〉

ＢＩＡ→ＩＴ　〈発行者バッチ要求〉

ＢＩＡ→ＩＴ　ＯＫ

ＢＩＡ／ＬＣＤ：〈私はＤＰＣ中央と対話している〉

ＩＴ→ＤＰＣ　〈発行者バッチ要求〉〈メッセージ鍵により暗号化された発行者バッチ〉

ＤＰＣ：ＢＩＡの識別に対してバイオメトリックの有効性を証明し、

銀行コードの有効性を証明する。

ＤＰＣ：秘密コードを取得する。

ＤＰＣ：メッセージ鍵を用いてメッセージを復号化し、発行者バッ

チを実行する。

ＤＰＣ→ＩＴ　〈発行者バッチ返答〉

ＩＴ→ＢＩＡ　応答を示せ〈発行者バッチ返答〉〈８〉

ＢＩＡ／ＬＣＤ：〈バッチＯＫ：私はそれを完全に信じる。（I am fully persuaded of it.）〉

ＢＩＡ→ＩＴ　〈ＯＫ〉

自動預金支払機（Automated Teller Machinery）

この場合、ＡＴＭは個人を識別し、銀行アカウント番号を取得するために、統合されたＡＴＭＢＩＡおよびＤＰＣと交信する。個人のアカウントは２１００－０２４５－３７７８－１２０１であり、銀行コードは２１００であり、個人の秘密コードは「私はそれを完全に信じる。（I am fully pursuaded of it.）」である。

ＡＴＭ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉

ＡＴＭ／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＡＴＭ　ＯＫ

ＡＴＭ／ＬＣＤ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はＡＴＭのキーボード上で１２３４５６を入力し、その後〈入力〉を押す。

ＡＴＭ→ＢＩＡ　ＰＩＮを設定せよ〈１２３４５６〉

ＢＩＡ→ＡＴＭ　ＯＫ

ＡＴＭ／ＬＣＤ：〈それではあなたのアカウント索引コードを入力し、その後〈入力〉を押して下さい。〉

個人は２を入力し、その後〈入力〉を入力する

ＡＴＭ→ＢＩＡ　アカウント索引コードを設定せよ〈２〉

ＢＩＡ→ＡＴＭ　ＯＫ

ＡＴＭ－）ＢＩＡ　レジスタを割り当てよ〈１〉〈２１００〉

ＢＩＡ→ＡＴＭ　ＯＫ

ＡＴＭ→メッセージを作成せよ〈アカウントアクセス〉

ＢＩＡ→ＡＴＭ　〈アカウントアクセス要求メッセージ〉

ＢＩＡ→ＡＴＭ　ＯＫ

ＡＴＭ／ＬＣＤ：〈私はＤＰＣ中央と対話している〉

ＡＴＭ→ＤＰＣ　〈アカウントアクセス要求メッセージ〉

ＤＰＣ：バイオメトリックの有効性を証明し、アカウント番号〉２１００　０２４５　３７７８　１２０１を取り出す。

ＤＰＣ：秘密コードを取得する。

ＤＰＣ→ＡＴＭ　〈アカウントアクセス応答メッセージ〉

ＡＴＭ→ＢＩＡ　応答を復号化せよ〈アカウントアクセス応答メッセージ〉

ＢＩＡ→ＡＴＭ　〈２１００－０２４５－３７７８－１２０１〉〈緊急ではない〉〈私はそれを完全に信じる。（I am fully persuaded of it.）〉

ＡＴＭ／ＬＣＤ：〈私はそれを完全に信じる。（I am fully persu-aded of it.）〉

この時点では、ＡＴＭは続ける必要があるアカウント番号を持っているため、アカウント番号に関連した情報を取り出し、個人との対話を始める。

電話ＰＯＳ端末（Phone Point of sale Terminal）

この場合、ＰＰＴは安全に電話を使って情報をダウンロードし、物品を購入するために、統合された電話ＢＩＡおよび電話マーチャントと交信する。個人のＰＩＣは１２３４であり、アカウント索引コードは１であり、マーチャントの電話番号は１　８００　５４２－２２３１であり、マーチャントコードは１２３４５６であり、実際のアカウント番号は４０２４－２２５６－５５２１－１２１２である。

ここで、電話が電話番号をシステムに渡す前に、電話番号から地域コード（１－８００）を取り除くことに注意すること。

個人は電話で１８００５４２２２３１をダイヤルする。

ＰＰＴ→マーチャント１８００５４２２２３１に接続する

ＰＰＴ→ＢＩＡ　レジスタを割り当てよ１〈５４２２２３１〉

販売データベース（Sales rep）は答える。個人は物品「フルーツケーキ」を選ぶ。販売データベースは情報をダウンロードする。

マーチャント→ＰＰＴ　〈１２３４５６　フルーツケーキ　４３．５４〉

ＰＰＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉

電話／ＬＣＤ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＰＰＴ　ＯＫ

電話／ＬＣＤ：〈あなたのＰＩＣを入力し、その後＃を押して下さい。〉

個人はキーパッド上で１２３４を入力し、その後＃又は＊（入力）を入力する。

ＰＰＴ→ＢＩＡ　ＰＩＮを設定せよ〈１２３４〉

ＢＩＡ→ＰＰＴ　ＯＫ

電話／ＬＣＤ：〈それではあなたのアカウント索引コードを入力して下さい。〉

個人は１を入力し、その後〈入力〉を入力する

ＲＰＴ→ＢＩＡ　アカウント索引コードを設定せよ〈１〉

ＢＩＡ→ＰＰＴ　ＯＫ

ＲＰＴ→ＢＩＡ　レジスタを割り当てよ〈２〉〈１２３４５６〉

ＢＩＡ→ＰＰＴ　ＯＫ

電話／ＬＣＤ：〈数量４５．５４でよければ＃を押して下さい。〉

個人は＃（はい）を入力する。

ＰＰＴ→ＢＩＡ　数量を設定せよ〈４３．５４〉

ＢＩＡ→ＰＰＴ　ＯＫ

ＰＰＴ→メッセージを作成せよ〈リモートトランザクション〉

ＢＩＡ→ＰＰＴ　〈リモートトランザクション要求〉

ＢＩＡ→ＰＰＴ　ＯＫ

電話／ＬＣＤ：〈私はＤＰＣ中央と対話している〉

ＰＰＴ→マーチャント　〈電話トランザクション要求〉

マーチャント→ＤＰＣ　ＤＰＣ公開鍵を用いて安全にＤＰＣに接続する。

マーチャント→ＤＰＣ　〈電話トランザクション要求〉

ＤＰＣ：バイオメトリックの有効性を証明し、アカウント番号を取り出す。→４０２４－２２５６－５５２１－１２１２

ＤＰＣ：マーチャント５４２２２３１がコード１２３４５６を有することの有効性を証明する。

ＤＰＣ→ＶＩＳＡ　〈４０２４－２２５６－５５２１－１２１２　４３．５４　１２３４５６を承認せよ〉

ＶＩＳＡ→ＤＰＣ　〈ＯＫ　承認コード４０２４－２２５６－５５２１－１２１２　４３．５４　１２３４５６〉

ＤＰＣ：秘密コードを取得する。

ＤＰＣ→マーチャント　〈トランザクション応答要求〉

マーチャントは応答コードを検査する。

マーチャント→ＰＰＴ　〈トランザクション応答メッセージ〉

ＰＰＴ→ＢＩＡ　応答を復号化せよ〈トランザクション応答メッセージ〉

ＢＩＡ→ＰＰＴ　〈ＯＫ　〈私はそれを完全に信じる。（I am fully persuaded of it.）〉　〈承認コード〉〉

電話／ＬＣＤ：〈チャイム〉トランザクションＯＫ：私はそれを完全に信じる。（I am fully persuaded of it.）

ケーブルテレビＰＯＳ端末（Cable-TV Point of sale terminal）

この場合、ＣＰＴは安全にケーブルテレビの広帯域ネットワークを使って情報をダウンロードし、物品を購入するために、統合されたケーブルテレビＢＩＡお

よび電話マーチャントと交信する。個人のＰＩＣは１２３４であり、アカウント索引コードは１であり、チャンネルは５であり、マーチャントコードは１２３４５６であり、実際のアカウント番号は４０２４－２２５６－５５２１－１２１２である。

個人はテレビのチャンネルを５に合わせる。

マーチャント→ＣＰＴ　〈フルーツケーキ　４３．５４　１２３４５６〉（放送）

個人はテレビのリモコン上の「買う」を押す。

ＣＰＴ／テレビ：〈フルーツケーキを４３．５４ドルで購入中〉

ＣＰＴ→ＢＩＡ　バイオメトリックを取得せよ〈２０〉

ＣＰＴ／テレビ：〈指を光っているパネルの上に置いて下さい。〉

個人は指をスキャナーの上に置く。

ＢＩＡ→ＣＰＴ　ＯＫ

ＣＰＴ／テレビ：〈あなたのＰＩＣを入力し、その後〈入力〉を押して下さい。〉

個人はキーパッド上で１２３４を入力し、その後「買う」を入力する。

ＣＰＴ→ＢＩＡ　ＰＩＮを設定せよ〈１２３４〉

ＢＩＡ→ＣＰＴ　ＯＫ

ＣＰＴ／テレビ：〈それではあなたのアカウント索引コードを入力して下さい。〉

個人は１を入力し、その後〈入力〉を入力する

ＲＰＴ→ＢＩＡ　アカウント索引コードを設定せよ〈１〉

ＢＩＡ→ＣＰＴ　ＯＫ

ＲＰＴ→ＢＩＡ　レジスタを割り当てよ〈１〉〈チャンネル５、１５：３０：　２０　ＰＳＴ〉

ＢＩＡ→ＲＰＴ　ＯＫ

ＣＰＴ→ＢＩＡ　レジスタを割り当てよ〈２〉〈１２３４５６〉

ＢＩＡ→ＣＰＴ　ＯＫ

　ＣＰＴ／テレビ：〈数量４５．５４でよければ「買う」を押して下さい。〉

　個人は「買う」を入力する。

ＣＰＴ－ＢＩＡ　数量を設定せよ〈４３．５４〉

ＢＩＡ→ＣＰＴ　ＯＫ

ＣＰＴ→メッセージを作成せよ〈ケーブルテレビトランザクション〉

ＢＩＡ→ＣＰＴ　〈ケーブルテレビトランザクション要求〉

ＢＩＡ→ＣＰＴ　ＯＫ

　ＣＰＴ／テレビ：〈私はＤＰＣ中央と対話している〉

ＣＰＴ→ＣＴＶセンター　〈ケーブルテレビトランザクション要求〉

ＣＴＶセンター→マーチャント　〈ケーブルテレビトランザクション要求〉

マーチャント→ＤＰＣ　ＤＰＣ公開鍵を用いて安全にＤＰＣに接続する。

　マーチャント＿ＤＰＣ　〈ケーブルテレビトランザクション要求〉

　ＤＰＣ：バイオメトリックの有効性を証明し、アカウント番号を取り出す。→４０２４－２２５６－５５２１－１２１２

　ＤＰＣ：チャンネル５で現在放映されているマーチャントがコード１２３４５６を有することの有効性を証明する。

ＤＰＣ→ＶＩＳＡ　〈４０２４－２２５６－５５２１－１２１２　４３．５４　１２３４５６を承認せよ〉

ＶＩＳＡ→ＤＰＣ　〈ＯＫ　承認コード４０２４－２２５６－５５２１－１２１２　４３．５４　１２３４５６〉

　ＤＰＣ：秘密コード、郵送先住所を取得する。

ＤＰＣ→マーチャント　〈トランザクション応答要求〉

　マーチャントは応答コードを検査し、郵送先住所を記録する。

マーチャント→ＣＴＶセンター　〈トランザクション応答メッセージ〉

ＣＴＶセンター→ＣＰＴ　〈トランザクション応答メッセージ〉

ＣＰＴ→ＢＩＡ　応答を復号化せよ〈トランザクション応答メッセージ〉

ＢＩＡ→ＣＰＴ　〈ＯＫ　〈私はそれを完全に信じる。（I am fully persuaded of it.）〉　〈承認コード〉〉

ＣＰＴ／テレビ：〈チャイム〉トランザクションＯＫ：私はそれを完全に信じる。（I am fully persuaded of it.）

前述の内容より、いかにして本発明の目的および特徴が実現されるかが評価されるであろう。

第一に、本発明は使用者がシステムアクセス要求を開始する目的で、トークンのような物理的な物体を所持し、提出する必要をなくすコンピューター識別システムを提供する。第二に、本発明は所有者の物体と情報を所持することを検証することに対向したものとして、使用者の同一性を検証することが可能なコンピューター識別システムを提供する。第三に、本発明は使用者にとって身体的に個人的な１以上の特徴に基づいて、使用者の同一性を検証する。第四に、本発明は承認されていない使用者による不正なアクセスの試みに対して高い抵抗性を有する、コンピューターシステムに安全にアクセスできるシステムを提供する。第五に、本発明は電子メッセージおよび／又はファクシミリの送り手と受け手の識別を可能にする識別システムを提供する。

本発明は特定のトークン不要の識別システムおよび方法に関して述べられているが、本発明から離れることなく装置および方法の様々な変形が可能であることは評価されるであろう。そして本発明は、以下に述べられた請求項により定義される。

用語解説

アカウント索引コード：

特定の金融資産アカウントに対応した単一の数字又は英数字の連続。

ＡＩＤ：

承認された個人データベース：個人および発行者ＢＩＡの装置を使用

するために承認された個人のリストを含む。

ＡＯＤ：

装置所有者データベース：各々のＢＩＡについての、地理的および接続の情報を含む中央データベース。

ＡＳＣＩＩ：

情報交換のためのアメリカ標準コード。

ＡＴＭ：

自動預金支払機：金融資産管理システムへのアクセスを行うために符号化されたバイオメトリック同一性情報を使用する。金融資産管理には、現金引き出し管理およびアカウント管理を含む。

ＢＩＡ：

バイオメトリック入力装置；バイオメトリック同一性情報を集め、それを符号化し暗号化する。またそれを承認できるようにする。異なるハードウェアのモデルおよびソフトウェアのバージョンが入ってくる。

バイオメトリック：

個人の身体的外観のいくつかの側面につきシステムにより行われる測定。

バイオメトリックＩＤ：

個人のバイオメトリック記録を独特に識別するためシステムにより用いられる識別子（ＩＲＩＤ－個人の記録ＩＤ）。

ＢＩＯ－ＰＩＣグループ：

同一の個人識別コードと連関した、アルゴリズム的に非類似のバイオメトリックのサンプル。

ＢＲＴ：

バイオメトリック登録端末；リテイルバンキングの出口に位置し、バイオメトリック登録情報を個人と結びつける。バイオメトリック登録情報は、選ばれたＰＩＮおよびシステムに個人を登録するための選ばれた個人情報である。

ＣＢＣ：

暗号ブロック連結；ＤＥＳのための暗号化モード。

ＣＣＤ：

荷電結合素子。

ＣＥＴ：

保証された電子メール端末;送り手を認識するためにＢＩＡを使用し、文書を暗号化し、システムに送信する。システムはシステム内のメッセージの到着を維持し、それを受け手に告知する。伝送装置への告知は、文書が送られると行われる。文書は検証されて送信され、ＢＩＡ暗号化により安全に保たれる。伝送装置は送信状況を調査することもある。参加者は両方ともシステムのメンバーでなければならない。

コマンド：

ＤＰＣ内て繰り返されるプログラム又はサブルーチンであり、特定のタスクを実行し、ＢＩＡを装備した端末から送られる要求メッセージによって活性化する。

契約受諾／拒否：

個人が自分のＢＩＯ－ＰＩＣを入力し、相手方の個人に電子ファクシミリで送信した文書内に含まれる、当該個人の契約の受諾又は拒否の単語を登録させるためにＤＰＣに命令する過程。

ＣＰＴ：

ケーブルテレビＰＯＳ端末：テレビの上のケーブルボックスに製品の映像とともに製品情報を知らせるデジタル信号を、同時放送するオンスクリーンディスプレイと、バイオメトリックＰＩＮ有効化をＣＡＴＶコミュニケーションネットワークを用いて実行するＢＩＡ制御リモコンを結合したもの。注文／承認／郵送先住所／物品ＩＤがマーチャントに送られる。承認の結果はテレビ上に表示される。

ＣＳＴ：

消費者サービス端末；アカウントの問題から人々を救うために、（アクセス特権に基づいて）アクセスの度合いを検査することで、個人の情報を取り出し、変形することができる能力をシステム消費者サービス職員に与える。

データシーリングステップ：

そのままのテキストを暗号テキストに変換すること（「暗号化」として知られる）。変換は、メッセージの暗号化されたチェックサム生成との組み合わせで行われる。いかなる実質的なメッセージの変形も検出する手段を同時に提供することにより、情報がそのままのテキストに残ることを可能にする。

ＤＥＳ：

デジタル暗号化標準:暗号によるデジタルデータの保護のための標準。標準ＡＮＳＩ　Ｘ３．９２－１９８１参照。

決定：

処理されて実行ステップ中にあるコマンドの状態。

ＤＰＣ：

データ処理センター。すなわち、複数ギガバイトのバイオメトリック同一性データベースをサポートする目標のために、ハードウェア、ソフトウェアおよび職員が配置されている場所および要素。ＤＰＣは電子メッセージを処理する。そして、ほとんどの電子メッセージは資金の移動、ファックスの送信、又は電子メールの送信のような何らかの行動を実行する準備としてバイオメトリック同一性検査の実行を包含する。

ＤＳＰ：

デジタル信号プロセッサ：集積回路の一分類であり、信号処理アプリケーションにより要求される数学的操作に特化している。

ＤＵＫＰＴ：

トランザクションについて固有の派生した鍵：標準ＡＮＳＩ／ＡＢＡ　Ｘ９．２４－１９９２参照。

ＥＤＤ：

電子文書データベース：すべての通信中のファックスおよび個人の読み取りを待っている電子メッセージを含む中央データベース。

緊急アカウント索引：

個人により選択される英数字又はその連続であって、アクセスされた時は、システムにより緊急トランザクションとしてラベル付けされたトランザクションとなる。潜在的には誤りスクリーンの表示、および／又は当該個人が伝送又はトランザクションの実行を強制された旨の承認の告知を引き起こす。

ＥＳＤ：

電子署名データベース：すべてのＭＤ５およびすべての文書のいかなる人により署名された電子署名も含む中央データベース。承認番号により参照される。

ＥＳＴ：

電子署名端末；個人の識別のためにＢＩＡを使用する。コンピューターは文書のチェックサムを計算し、システムにチェックサムを送る。システムは有効化し、タイムスタンプを付し、チェックサムを保存し、署名コード（sig code）とともに返す。通信手段としてインターネットを

使用する。ＥＳＴはまた署名コードおよびＭＤ５計算を与えられた署名を検証する。

ＦＡＲ（誤り受け取り率）：

ある個人のバイオメトリックが誤って他の個人のバイオメトリックとして識別される統計的近似値。

誤りスクリーン：

微妙に不正確になるように意図的に予め決められた情報の表示であり、他人が情報の変化を知らないでいる限り、他人に違法に個人の金融資産についての正確なデータを得させないようにしている。

ＦＤＤＩ：

ファイバーデジタル機器インターフェース：ファイバー光トークンリングを使えるようにするためのネットワーク機器。

ＦＳ：

フィールドセパレータ。

ＦＷ：

ファイアウォール機器：ＤＰＣに入り、ＤＰＣから出るトラフィックを規制するインターネットルータ。

ＧＭ：

ゲートウェイ機器：ＤＰＣ内の主要処理コンピュータであり、ほとんどのソフトウェアを動作させる。

ＩＢＤ：

個人バイオメトリックデータベース：バイオメトリック、金融資産、および他の個人情報のための中央データベース。バイオメトリックデータベースに対する調査はトランザクション承認および伝送のために用いられる。

ＩＤ：

発行者データベース：金融資産アカウント番号を追加し、削除することを許可する構成を含む中央データベース。

ＩＭＬ：

ＩＢＤ機器リスト：どのＩＢＤ機器がどのＰＩＮコードに対応できるかを決定するソフトウェアモジュール。

インターネットマーチャント：

インターネット電子ネットワークの手段によりサービス又は物を消費者に売るリテールアカウント。

ＩＰＴ：

インターネットＰＯＳ端末：インターネットからの品目およびマーチャントコード、有効化のためのＢＩＡバイオメトリックＰＩＮをインターネットを使ってシステムに送信し、承認／注文／ＰＯ＃をマーチャン

トに転送する。システムもインターネットを使って応答し、結果をスクリーンに表示する。

発行者：

ＤＰＣで登録される金融資産のための金融アカウント発行者。

発行者バッチ：

ＤＰＣに対する発行者によって検証され、入力されるバイオメトリックＩＤ、金融資産アカウント、アカウント索引コードと共に完成する

「追加」および「削除」命令の集まり。

ＩＴ：

発行者端末；特定の個人のＩＢＤ記録から（彼ら自身の）金融資産アカウント番号を追加し、削除するために、システムに関連あるバッチを発行者に提供する。

ＩＴＴ：

インターネット対話端末；バイオメトリックＩＤを用いてＤＰＣから得られる暗号化された証明書を使って、ネットワーク端末セッションを承認する。

ＬＣＤ：

液晶ディスプレイ：テキストを表示するために用いられる技術。

ＭＡＣ：

メッセージ承認コード：暗号化チェックサムアルゴリズム。ＭＡＣはＭＡＣの計算後変更されていないメッセージの内容に保証を与える。ＡＮＳＩ　Ｘ９．９－１９８６参照。

ＭＡＣＭ：

メッセージ承認コードモジュール：行きおよび帰りのパケットのためのＭＡＣが行う有効化および生成を扱うＤＰＣ内のソフトウェアモジュール。

ＭＤＭ：

メッセージ復号化モジュール：ＢＩＡ機器からの、あるいはＢＩＡ機

器へ向かうパケットを暗号化し、復号化するＤＰＣ内のソフトウェアモジュール。

ＭＰＭ：

メッセージ処理モジュール：要求パケットの処理を行うＤＰＣ内のソフトウェアモジュール。

ネットワーククリデンシャル：

個人と銀行の双方がＤＰＣによりネットワーククリデンシャルを作るために識別される。証明書は接続の状況（例えば、ＴＣＰ／ＩＰソース・ディスティネーションポート）と共に、個人の識別を含む。ＤＰＣは個人のアカウントＩＤ、時刻および銀行コードを用いてネットワーククリデンシャルを作る。ＤＰＣは公開鍵による暗号化およびＤＰＣの秘密鍵を用いてこのクリデンシャルに署名する。

ＰＦＤ：

以前の詐欺行為データベース：関連して詐欺行為があったＩＢＤ記録のための中央データベース。すべての新しい消費者のバイオメトリックスは、常習犯を減らすために全てのＰＦＤ記録に対して検査される。

ＰＧＬ：

ＰＩＮグループリスト：ＩＢＣ機器の構成を維持するために責任を有するＤＰＣ内のソフトウェアモジュール

ＰＩＮ：

個人識別番号；少なくとも１つの番号からなる秘密の知識を通じて、個人のアカウントに対するアクセスを防止する方法。

ＰＩＣ：

個人識別コード；数字、記号又はアルファベット文字から作成されるＰＩＮ。

ＰＯＳ：

ポイント・オブ・セール；物が売られる場所。

ＰＰＴ：

電話ＰＯＳ端末；ＢＩＡを装備した電話を通じてのトランザクションを承認するため、電話番号をマーチャントの価格・製品情報に結合させる。

注文／承認／郵送先住所／ＰＯはマーチャントに転送される。承認の結果は個人の秘密コードとともに電話のＬＣＤ上に表示され、又は「話される」。

ＲＡＭ：

ランダムアクセスメモリ。

ＲＦ：

無線周波数：一般に電気機器の通常動作中に放出される高周波エネルギーのことをいう。

レジスタ：

特定の目的、データのために予約されるメモリ。集積回路の脇に置かれ、命令に対してオペランドを蓄える。

要求：

ＢＩＡからＤＰＣに対しての電子命令であり、ＤＰＣに個人を識別し、その後識別に成功すれば個人のコマンドを処理するように命令する。

ＲＭＤ：

遠隔マーチャントデータベース：マーチャントの電話と、ケーブルテレビ注文店についての、マーチャントＩＤで索引付けされたすべてのマーチャントの識別コードを含む。マーチャントごとのシステムの暗号化コードも含む。

ＲＰＴ：

リテールＰＯＳ端末；暗号化されたバイオメトリック同一性情報を、リテールトランザクション情報（現金レジスターからの情報の場合もある）に結合させる。また、システムの承認要求をＸ．２５ネットワーク、モデム等を使って案出する。

安全伝送：

少なくとも一人の参加者がＤＰＣに識別されている場合における電子メッセージ又はファクシミリ。

ＳＦＴ：

安全ファックス端末；送り手を識別するためにＢＩＡを用いる。安全にされていないファックス、送り手により安全にされているファックス、安全にされているファックス、証明書により安全にされているファックスのいずれも送信する。後者の２つについては、受け手がバイオメトリックＰＩＮを用いて自分自身を識別することが要求される。行きのファックスをラベル付けするために「タイトル」（タイトル索引数字を用いて特定される）を用いる。送り手は伝達状況を調べることもある。双方の参加者はシステムのメンバーでなければならない。送り手と受け手のいずれもがファックスが実現されることを要求できる。

ＳＮＭ：

連続番号モジュール：帰りの要求パケットのためのＤＵＫＰＴ連続番号処理を扱うＤＰＣ内のソフトウェアモジュール。連続番号処理は再試行（replayattacks）を防止する。

端末：

バイオメトリックサンプルを集め、要求メッセージを形成するためにＢＩＡを使用する装置。要求メッセージはその後承認および実行のためにＤＰＣに送信される。端末はほとんど常に、要求メッセージに相手方および同様の者を識別する補助的な情報を付加する。

タイトル索引コード：

個人の承認された役割又は能力を、その個人の職業の状況と共に固有に識別する英数字の連続。

トークン：

能力を与える動かない物体。

トラッキングコード：

ＤＰＣにより蓄積され又は伝送されたデータに割り当てられた英数字の連続。連続は、データを回復（recall）し、データ伝送の状態についての報告を得るために用いられることもあるように、割り当てられている。

トランザクション：

電子による金融の取引。

伝送：

電子による金融の取引以外の電子のメッセージ（message）。

ＶＡＤ：

有効装置データベース：ＢＩＡの所有者に加えて、各々のＢＩＡ（関連する特有の暗号化コードとともに）が認識される、中央データベース。

【図１】

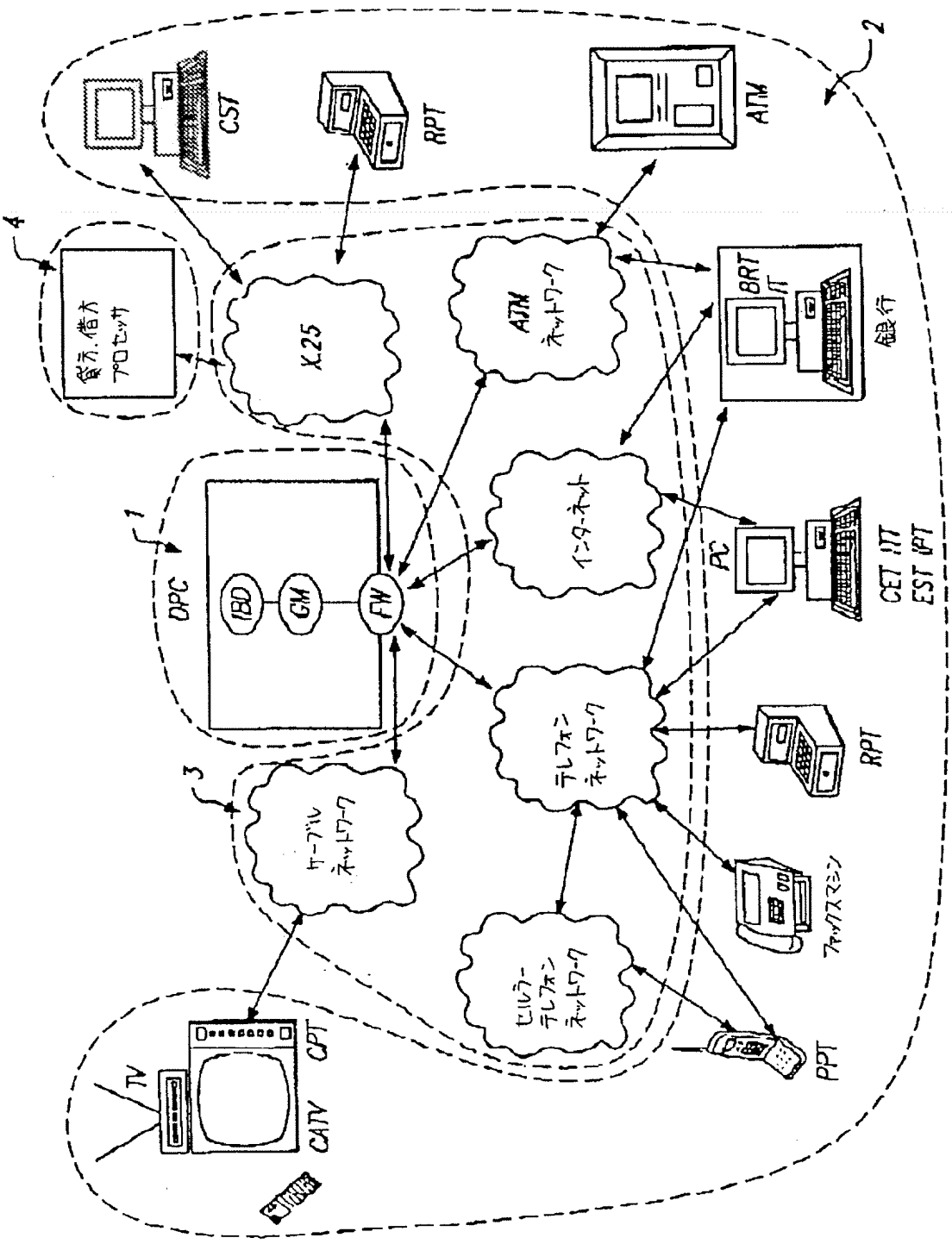
CST
RPT
ATM
2
4
貸方.借方
プロセッサ
X.25
ATM
ネットワーク
BRT
IT
銀行
1
DPC
IBD
GM
FW
インターネット
PC
CET ITT
EST IPT
テレフォン
ネットワーク
RPT
3
ケーブル
ネットワーク
ファックスマシン
セルラー
テレフォン
ネットワーク
PPT
CPT
TV
CATV

FIG. 1

【図２】

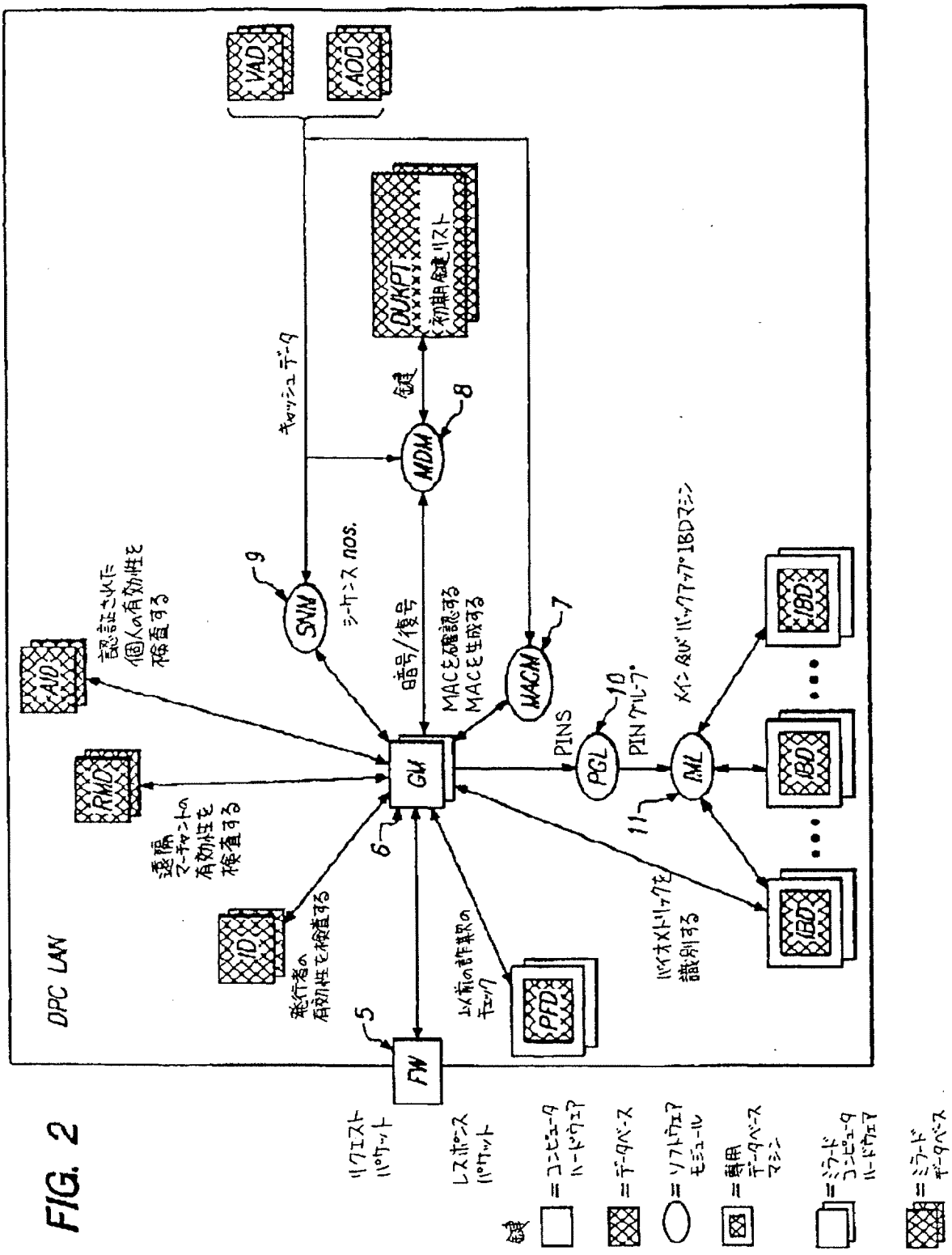
VAD
AAD
DUKPT 初期鍵リスト
鍵
MDM
8
キャッシュデータ
SNM
9
シーケンス nos.
暗号/復号
MACと確認する
MACを生成する
MACM
7
AID
認証された人の個人の有効性を検査する
RMD
透隔マーチャントの有効性を検査する
ID
発行者の有効性を検査する
GW
6
PINS
PGL
10
PIN プル-ア°
IML
11
メイン & バックアップ IBDマシン
IBD
IBD
IBD
バイオメトリックを識別する
PFD
以前の許可のチェック
FW
5
DPC LAN
リクエスト パケット
レスポンス パケット
鍵
= コンピュータ ハードウェア
= データベース
= ソフトウェア モジュール
= 専用 データベース マシン
= ミラード コンピュータ ハードウェア
= ミラード データベース

FIG. 2

【図３】

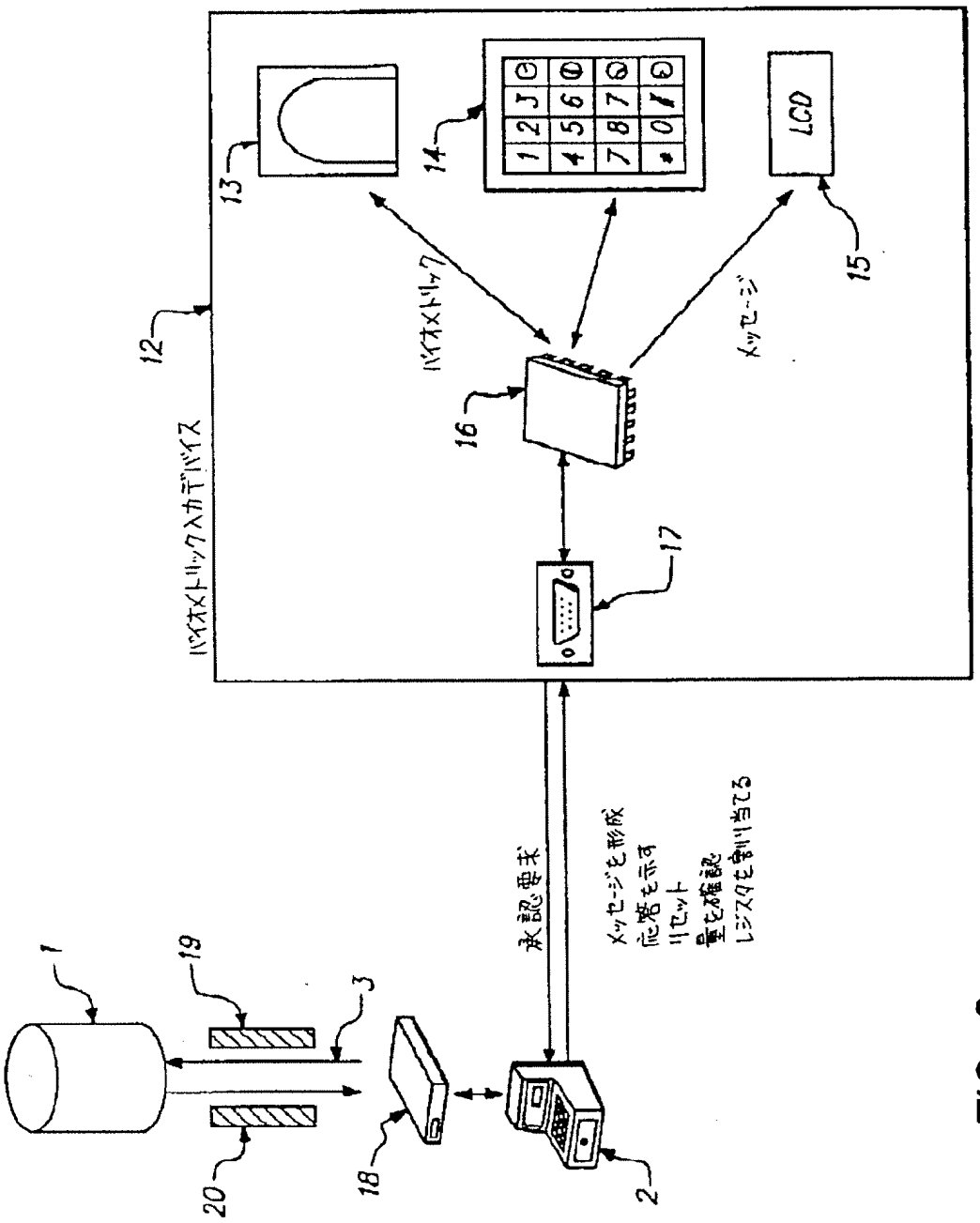
12
13
14
15
16
17
18
19
20
1
2
3
LCD
承認要求
メッセージを形成
応答を示す
リセット
量を確認
レジスタを割り当てる

FIG. 3

【図４】

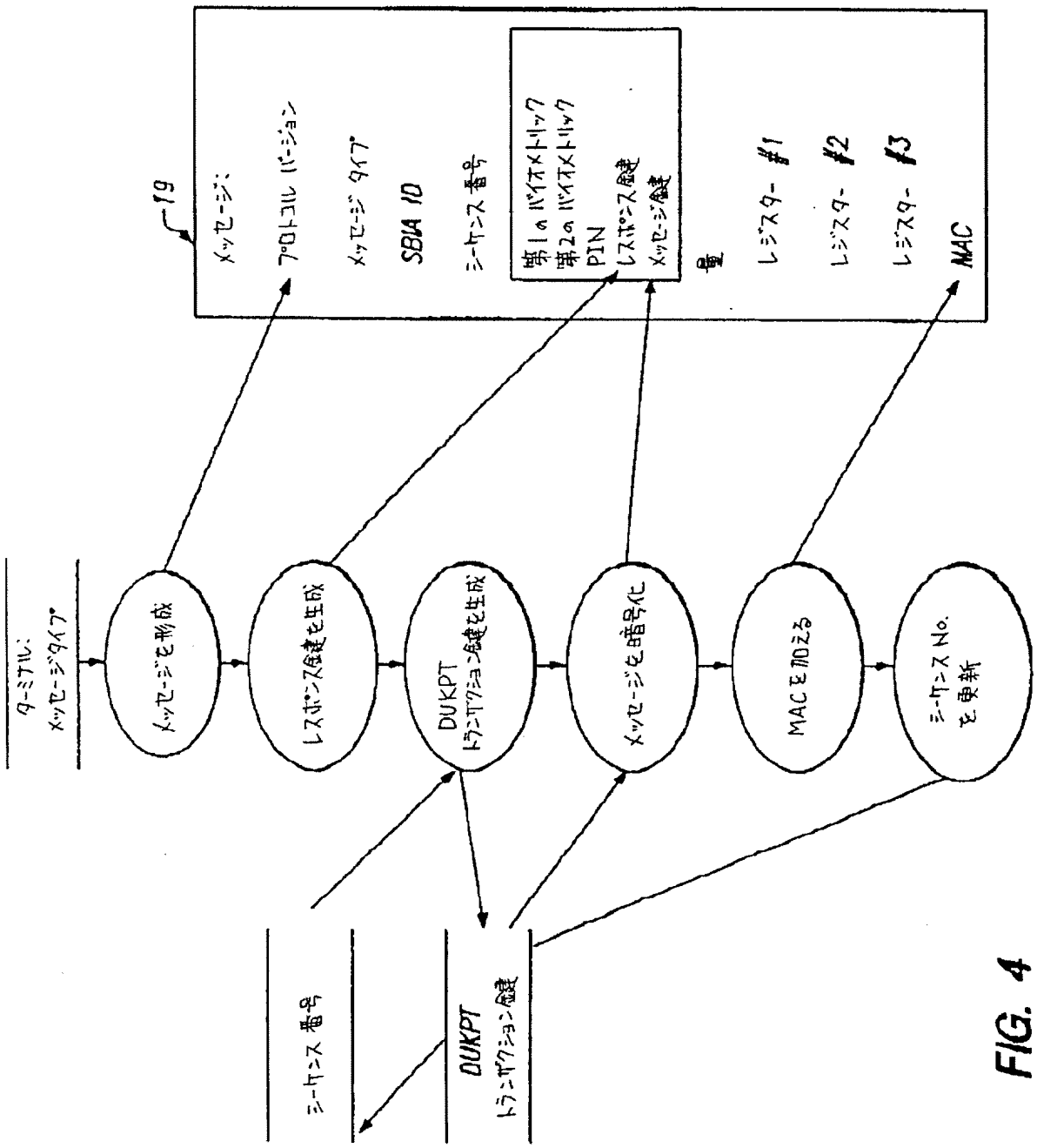
19
メッセージ:
プロトコル バージョン
メッセージ タイプ
SBIA ID
シーケンス番号
第1のバイオメトリック
第2のバイオメトリック
PIN
レスポンス鍵
メッセージ鍵
量
レジスター #1
レジスター #2
レジスター #3
MAC
ターミナル:
メッセージタイプ
メッセージを形成
レスポンス鍵を生成
DUKPT
トランザクション鍵を生成
メッセージを暗号化
MACをかける
シーケンスNo.
を更新
シーケンス番号
DUKPT
トランザクション鍵

FIG. 4

【図５】

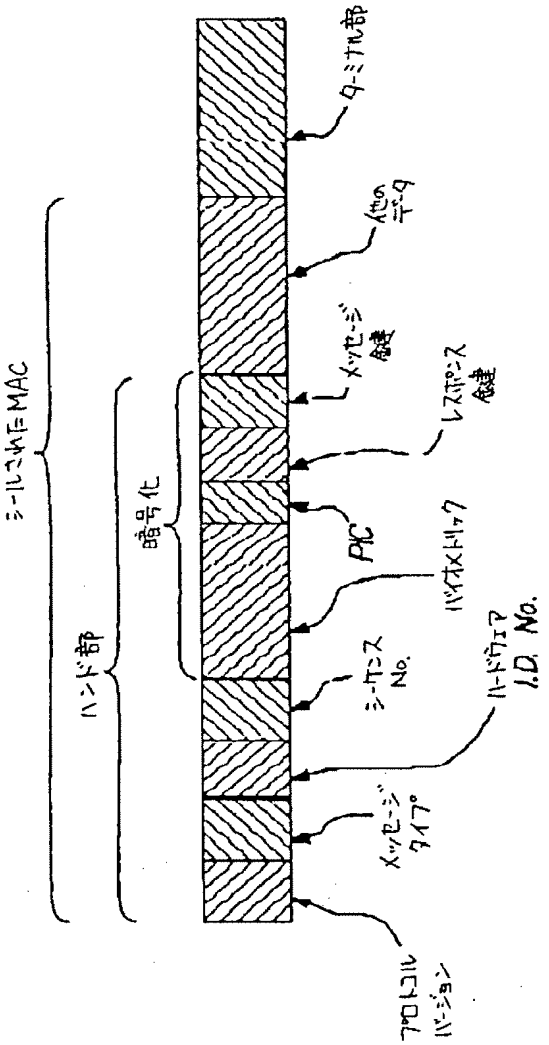
ターミナル部
メッセージ長
メッセージ鍵
レスポンス鍵
PIC
バイオメトリック
ハードウェア I.D. No.
シーケンス No.
メッセージタイプ
プロトコルバージョン
暗号化
ハンド部
シールMAC

FIG. 5

【図６】

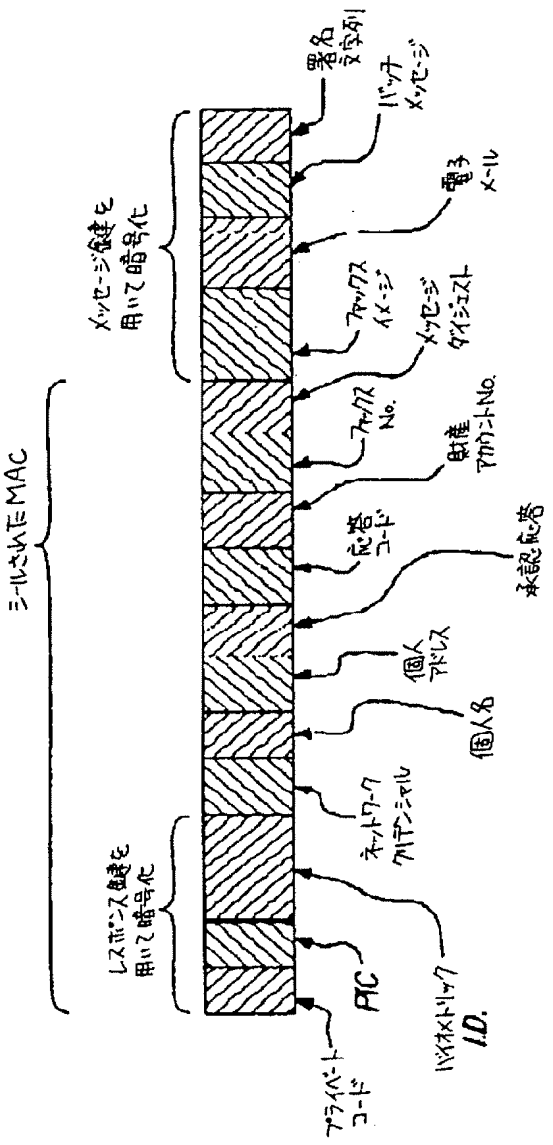
署名
バッチ
メッセージ
電子
メール
メッセージ
ダイジェスト
No.
No.
応答
コード
承認応答
個人
アドレス
個人名
ネットワーク
アドレス
PIC
I.D.
プライベート
コード
メッセージ鍵を
用いて暗号化
シールされたMAC
レスポンス鍵を
用いて暗号化

FIG. 6

【図７】

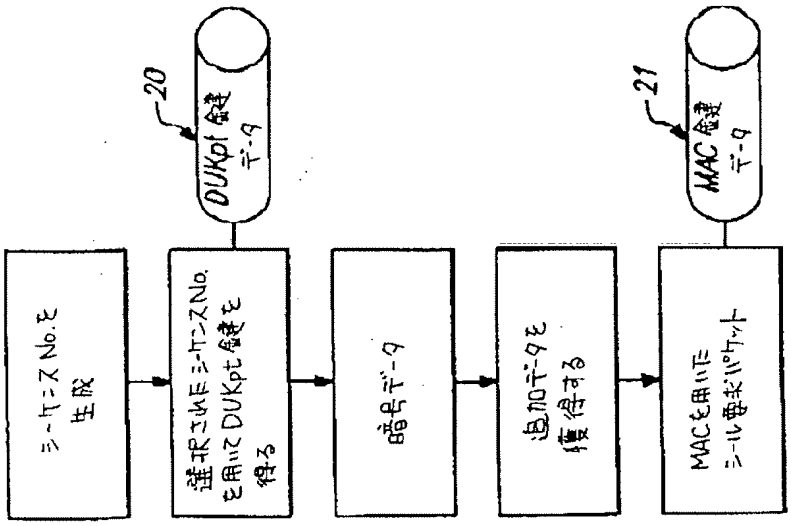

FIG. 7

【図８】

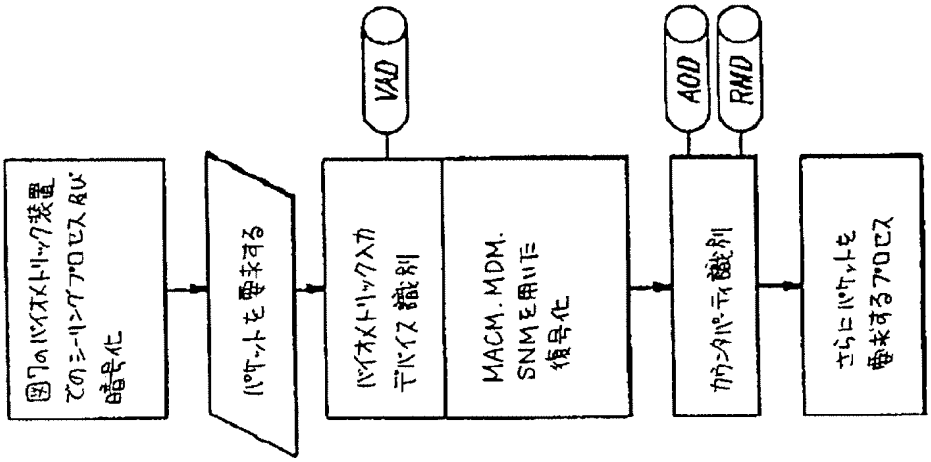

FIG. 8

【図９】

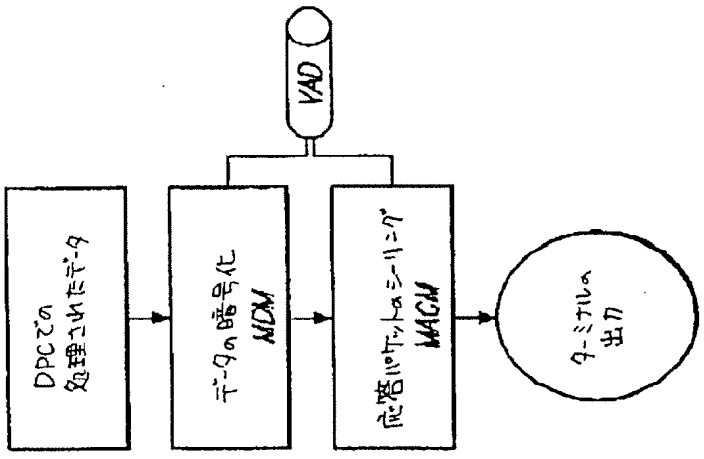

FIG. 9

【図１０】

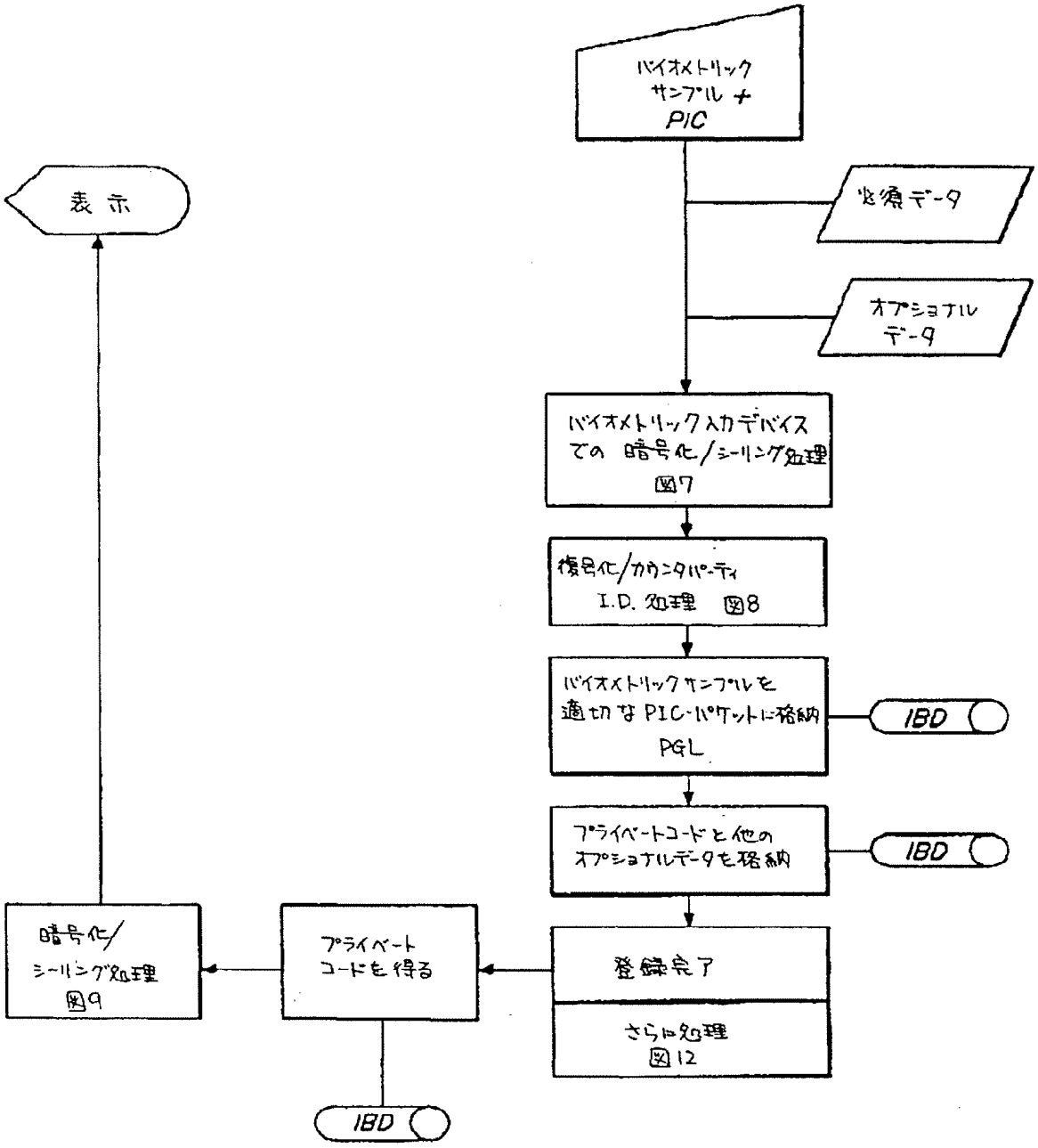
バイオメトリック
サンプル＋
PIC
必須データ
オプショナル
データ
バイオメトリック入力デバイス
での 暗号化/シーリング処理
図7
復号化/カウンタパーティ
I.D. 処理 図8
バイオメトリックサンプルを
適切な PIC-パケットに格納
PGL
IBD
プライベートコードと他の
オプショナルデータを格納
IBD
登録完了
さらに処理
図12
プライベート
コードを得る
暗号化/
シーリング処理
図9
表示
IBD

Fig .01

【図１１】

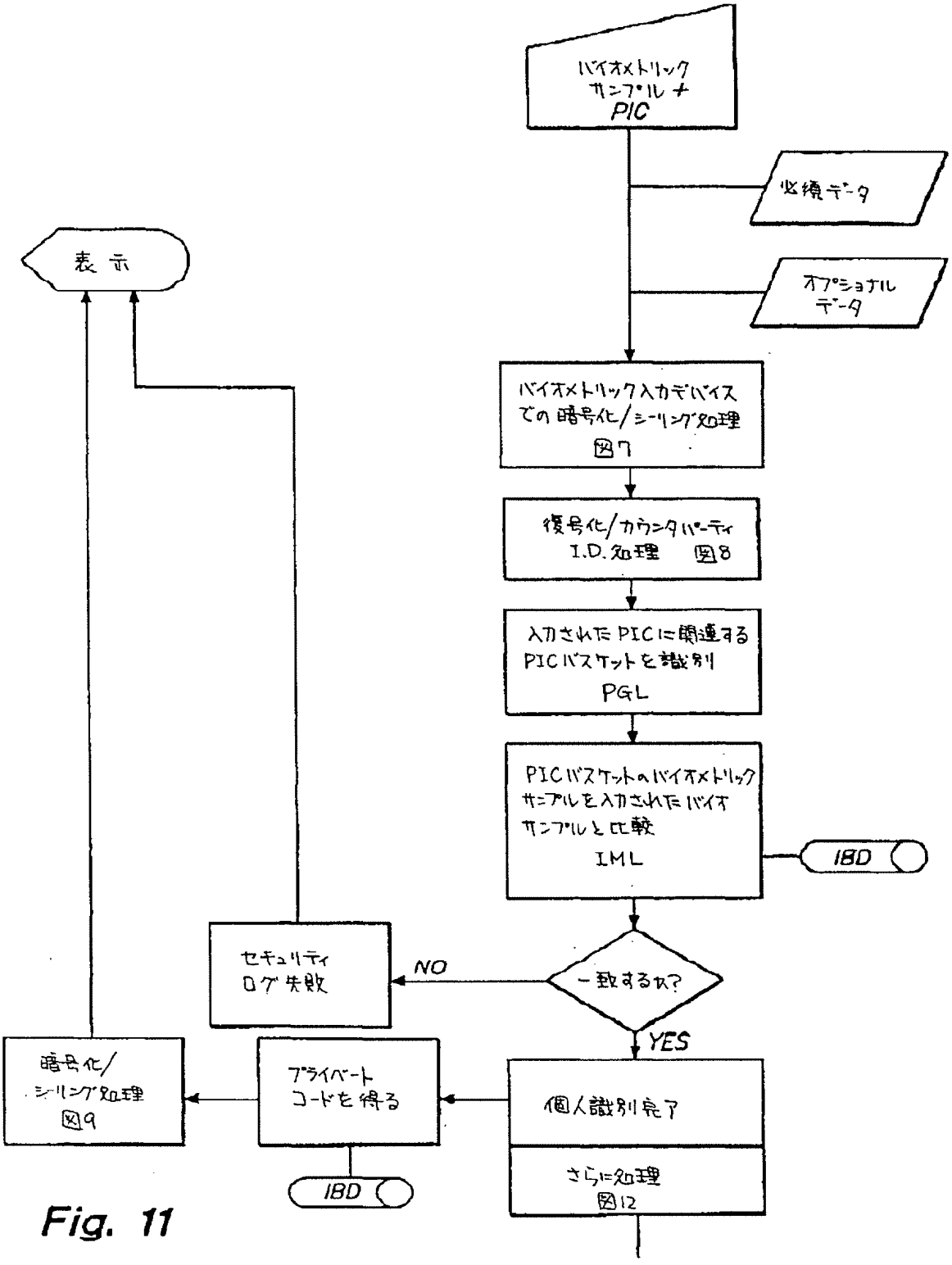
バイオメトリック
サンプル＋
PIC
必須データ
オプショナル
データ
表示
バイオメトリック入力デバイス
での暗号化/シーリング処理
図7
復号化/カウンタパーティ
I.D.処理 図8
入力されたPICに関連する
PICバスケットを識別
PGL
PICバスケットのバイオメトリック
サンプルを入力されたバイオ
サンプルと比較
IML
IBD
一致するか?
NO
YES
セキュリティ
ログ失敗
暗号化/
シーリング処理
図9
プライベート
コードを得る
個人識別完了
さらに処理
図12
IBD

Fig. 11

【図１２】

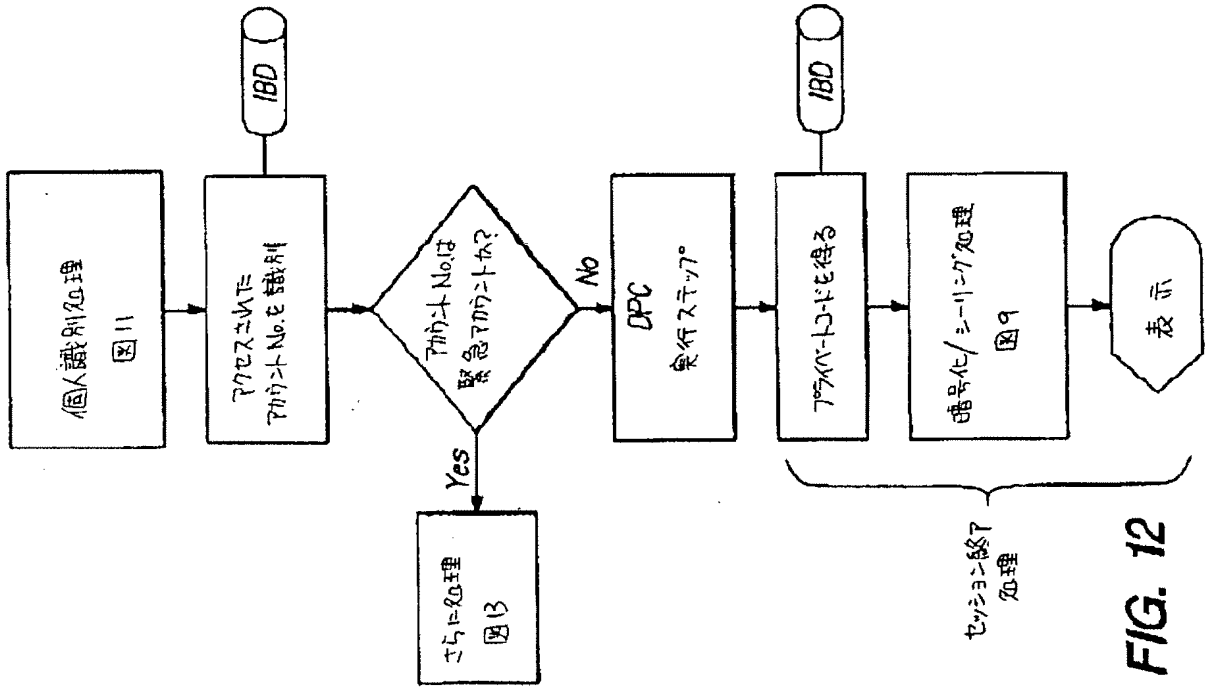

FIG. 12

【図１３】

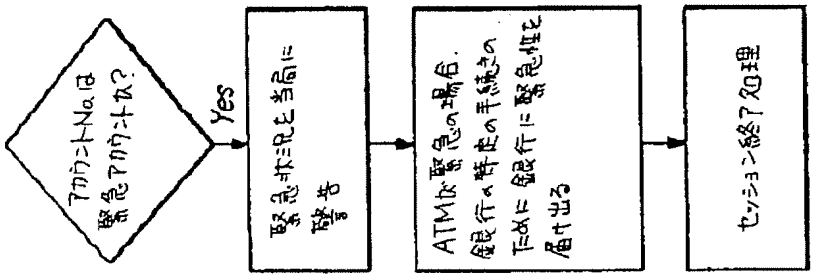

FIG. 13

【図１４】

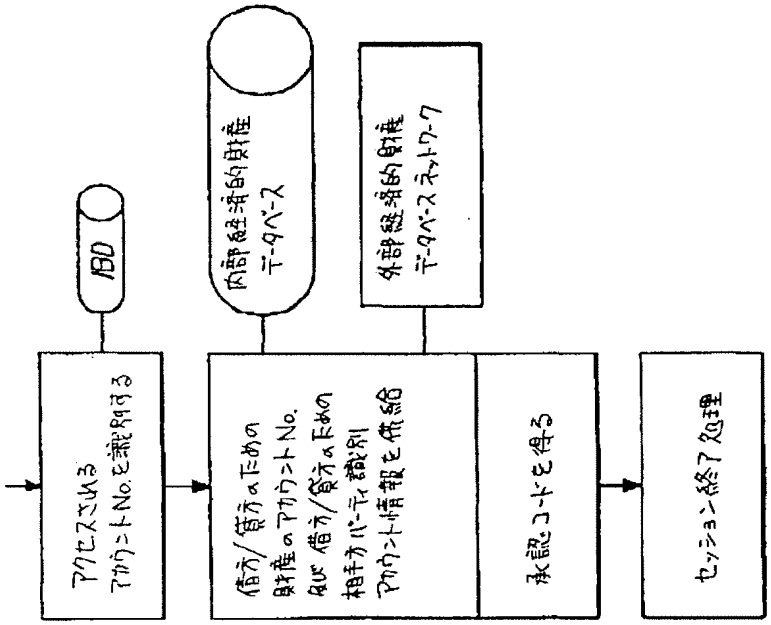

FIG. 14

【図１５】

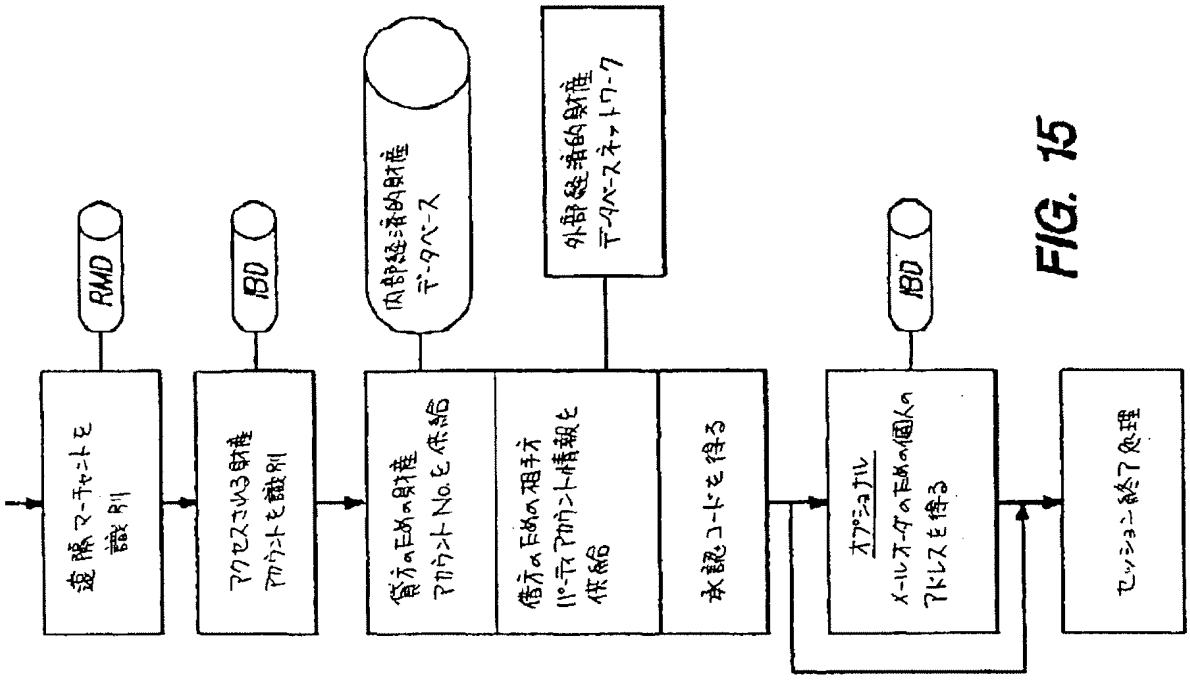

FIG. 15

【図１６】

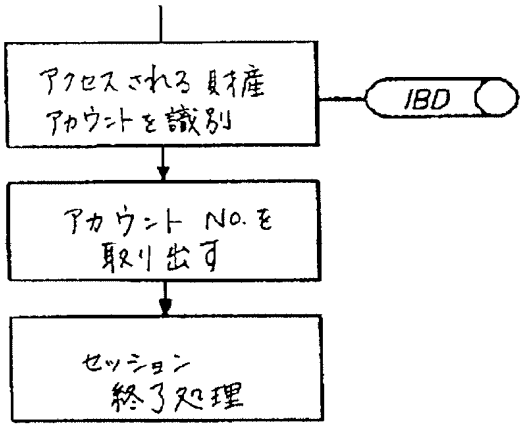

FIG. 16

【図１７】

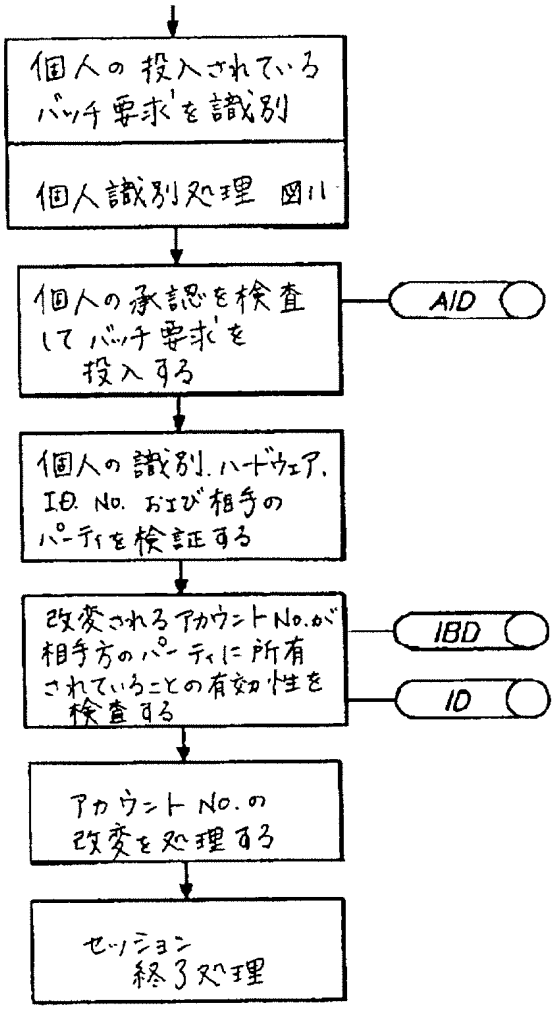

FIG. 17

【図１８】

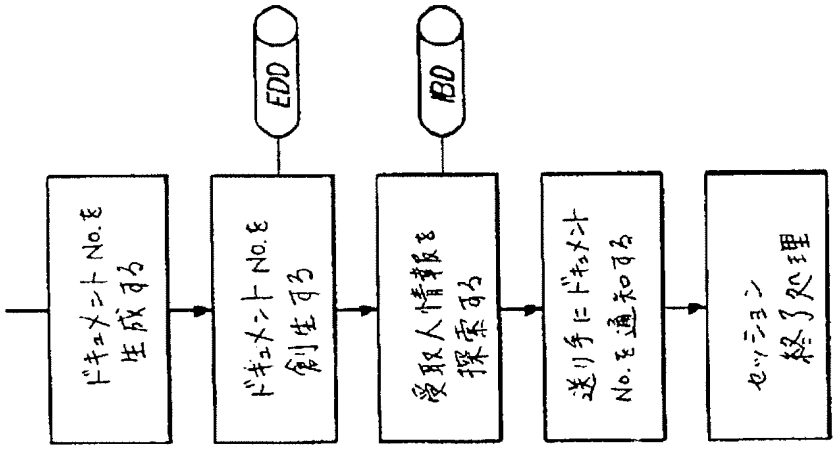

FIG. 18

【図１９】

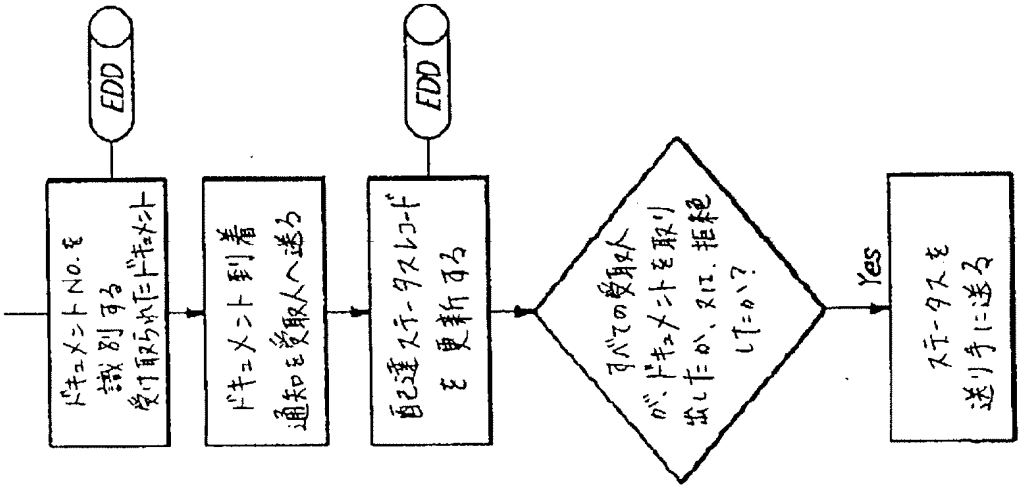
EDD
ドキュメントNo.を
識別する
受け取られたドキュメント
ドキュメント到着
通知を受取人へ送る
EDD
配達ステータスレコード
を更新する
全ての受取人
がドキュメントを取り
出したか、又は、拒絶
したか?
Yes
ステータスを
送り手に送る

FIG. 19

【図２０】

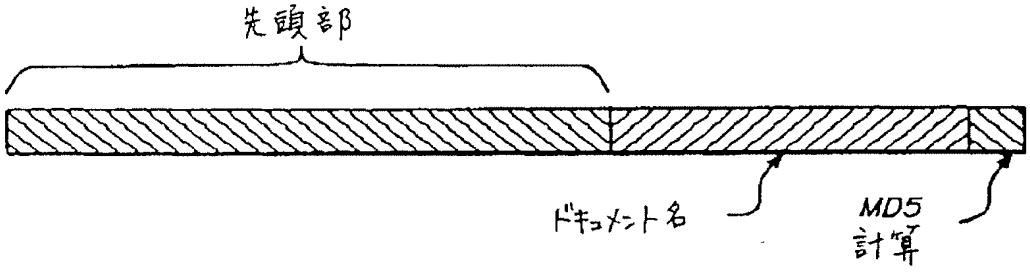

FIG. 20A

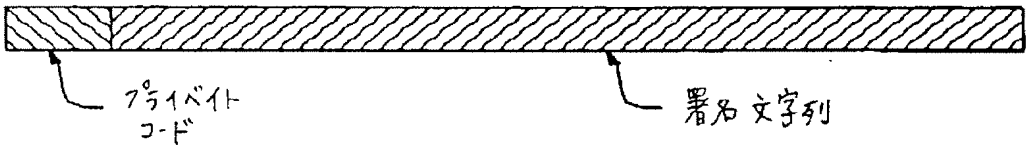

FIG. 20B

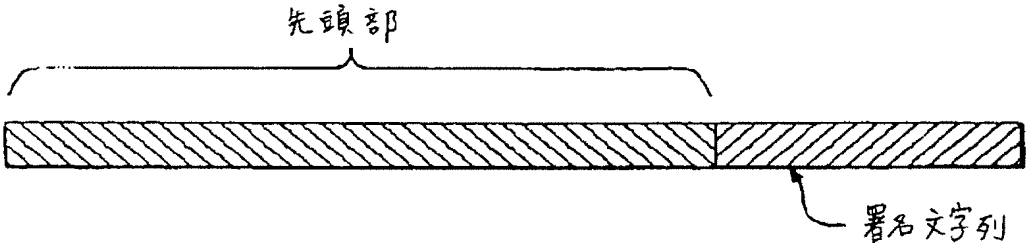

FIG. 20C

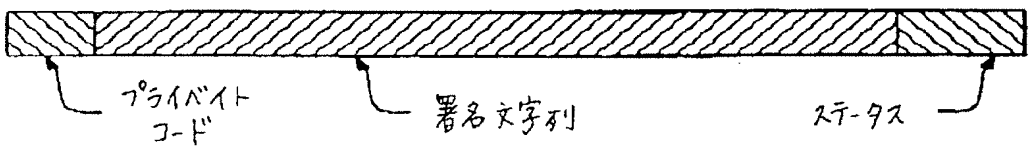

FIG. 20D

【図２１】

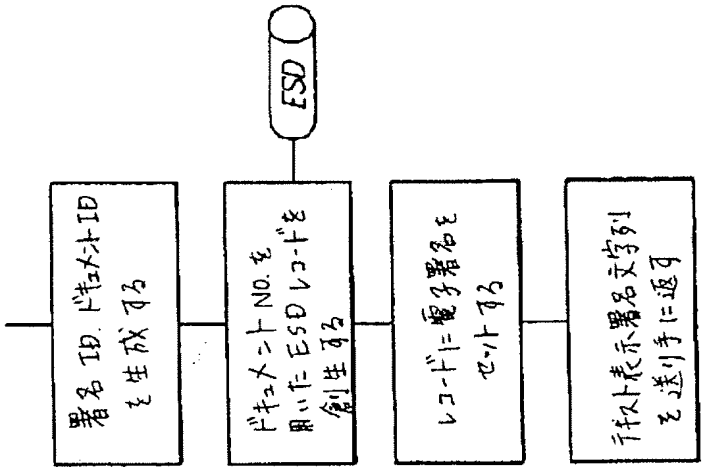

FIG. 21

【図２２】

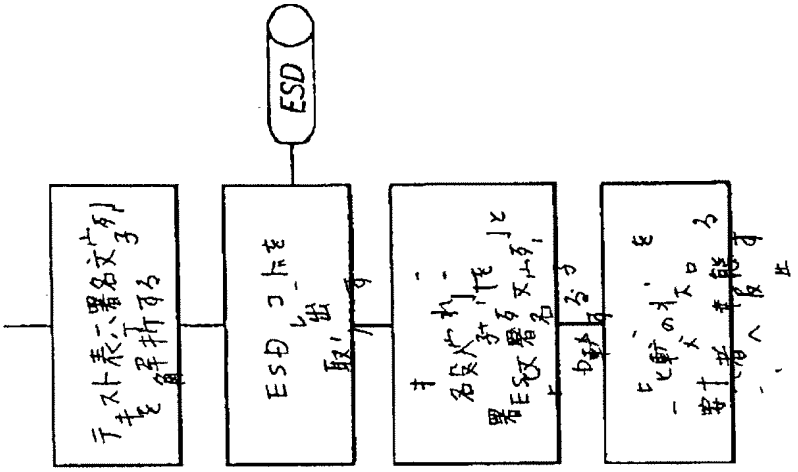

FIG 2

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G06K 9/00
US CL :Please See Extra Sheet.
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,229,764 (MATCHETT ET AL) 20 July 1993, see abstract, figure 1, column 1, lines 6-59, column 8, lines 19-25.	1-87
Y	US, A, 5,191,611 (LANG) 02 March 1993, column 16, line 27.	1-87

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be part of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 JULY 1996	26 AUG 1996
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer LEO BOUDREAU Telephone No. (703) 308-7595

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

フロントページの続き

(81)指定国　　ＥＰ(ＡＴ，ＢＥ，ＣＨ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＦＲ，ＧＢ，ＧＲ，ＩＥ，ＩＴ，ＬＵ，ＭＣ，ＮＬ，ＰＴ，ＳＥ)，ＯＡ(ＢＦ，ＢＪ，ＣＦ，ＣＧ，ＣＩ，ＣＭ，ＧＡ，ＧＮ，ＭＬ，ＭＲ，ＮＥ，ＳＮ，ＴＤ，ＴＧ)，ＡＰ(ＫＥ，ＬＳ，ＭＷ，ＳＤ，ＳＺ，ＵＧ)，ＡＭ，ＡＴ，ＡＵ，ＢＢ，ＢＧ，ＢＲ，ＢＹ，ＣＡ，ＣＨ，ＣＮ，ＣＺ，ＤＥ，ＤＫ，ＥＳ，ＦＩ，ＧＢ，ＧＥ，ＨＵ，ＪＰ，ＫＥ，ＫＧ，ＫＰ，ＫＲ，ＫＺ，ＬＫ，ＬＴ，ＬＵ，ＬＶ，ＭＤ，ＭＧ，ＭＮ，ＭＷ，ＭＸ，ＮＯ，ＮＺ，ＰＬ，ＰＴ，ＲＯ，ＲＵ，ＳＤ，ＳＥ，ＳＩ，ＳＫ，ＴＪ，ＴＴ，ＵＡ，ＵＺ，ＶＮ

(72)発明者　リー，ジョナサン　エイ．
アメリカ合衆国　カリフォルニア　94704，
バークレー，シャタック　スクエア　46，
スイート　12